ISACA

Updated for 2019 Job Practice

CISA®

Review Manual

27th Edition

CISA Certified Information Systems Auditor®
An ISACA® Certification



ISACA®

Updated for 2019 Job Practice

CISA®

Review Manual

27th Edition

CISA® Certified Information Systems Auditor®

An ISACA® Certification



About ISACA

Now in its 50th anniversary year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations.

Among those credentials, ISACA advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified in Risk and Information Systems Control™ (CRISC™), Certified Information Security Manager® (CISM®) and Certified in the Governance of Enterprise IT® (CGEIT®) credentials.

ISACA leverages the expertise of its 460,000 engaged professionals—

including its 140,000 members—in information and cybersecurity,

governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 220 chapters worldwide and offices in both the United States and China.

Disclaimer

ISACA has designed and created *CISA® Review Manual 27th Edition* primarily as an educational resource to assist individuals preparing to take the CISA certification exam. It was produced independently from the CISA exam and the CISA Certification Committee, which has had no responsibility for its content. Copies of past exams are not released to the public and were not made available to ISACA for preparation of this publication. ISACA makes no representations or warranties whatsoever with regard to these or other ISACA publications assuring candidates' passage of the CISA exam.

Reservation of Rights

© 2019 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval

system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA.

ISACA

1700 E. Golf Road, Suite 400

Schaumburg, IL 60173 USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Contact us: https://support.isaca.org

Website: www.isaca.org

Participate in the ISACA Online Forums:

https://engage.isaca.org/onlineforums

Twitter: www.twitter.com/ISACANews

LinkedIn: www.linkd.in/ISACAOfficial

Facebook: www.facebook.com/ISACAHQ

Instagram: www.instagram.com/isacanews

ISBN 978-1-60420-767-5

CISA® Review Manual 27th Edition

CRISC is a trademark/service mark of ISACA. The mark has been applied for or registered in countries throughout the world.

CISA Review Manual 27th Edition

ISACA is pleased to offer the 27th edition of the *CISA® Review Manual*. The purpose of this manual is to provide Certified Information Systems Auditor (CISA) candidates with the technical information and reference material to assist in preparation for the Certified Information Systems Auditor exam.

The content in this manual is based on the CISA Job Practice, available at

www.isaca.org/cisajobpractice. **This job practice is the basis for the CISA exam.** The development of the job practice involves thousands of CISA-certified individuals and other industry professionals worldwide who serve as committee members, focus group participants, subject matter experts and survey respondents.

The *CISA® Review Manual* is updated to keep pace with rapid changes in the information systems (IS) audit, control and security professions. As with previous manuals, the 27th edition is the result of contributions from many qualified authorities who have generously volunteered their time and expertise. We respect and appreciate their contributions and hope their efforts provide extensive educational value to *CISA® Review Manual* readers.

Certification has positively impacted many careers; the CISA designation is respected and acknowledged by organizations around the world. We wish you success with the CISA exam. Your commitment to pursue the leading certification in IS audit, assurance, control and security is exemplary.

Acknowledgments

The 27th edition of the *CISA® Review Manual* is the result of the collective efforts of many volunteers. ISACA members from throughout the global IS

audit, control and security professions participated, generously offering their talent and expertise. This international team exhibited a spirit and selflessness that have become the hallmark of contributors to this manual. Their participation and insight are truly appreciated.

Special thanks to Pamela J. Nigro, CISA, CGEIT, CRISC, Senior Director GRC, Information Security, Health Care Service Corporation, USA; Deborah A. Oetjen, USA; and Terry Trsar, USA, for their assistance in developing the content for the update.

Contributors

Ian Cooke, CISA, CRISC, CGEIT, CIPT, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green

Belt, An Post, Ireland

Zou Guodong, CISA, CISM, CGEIT, CRISC, China

Rudy Matiska, CISA, PwC, USA

Patricia North-Martino, CISA, MSCIS, USA

Pavel Strongin, CISA, CISM, CPA, USA

Lisa Fengping Yip, CISA, USA

Expert Reviewers

Sanjiv Agarwala, MD, CISA, CISM, CGEIT, Oxygen Consulting Services Pvt Ltd, India

Akinwale Akindiya, CISA, ACA, Royalway Consulting, Nigeria

Sunil Bhaskar Bakshi CISA, CISM, CGEIT, CRISC, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP, India

Konstantinos Baliotis, CISA, Greece

Zsolt Bederna, CISA, CISM, CGEIT, C|EH, CISSP, ITIL 2011 Foundation, TOGAF 9 Foundation, Hungary

Anupma Bhatia, CISA, CRISC, USA

Ishwar Chandra, CISA, FCA, IC & Associates, Chartered Accountants, India
Mouhamed Diop, CISA, CISM, CGEIT, CRISC, Senegal

Ahmad ElGhazouly, DBA, CISA, CISM, CRISC, ACP, PBA, PMP, RMP,

TOGAF, PGESCo, Egypt

Marco Ermini, PhD, CISA, CISM, CISSP, ITILv3, GCIH, RCSS, Germany
Shigeto Fukuda, CISA, EYACC, Japan

Sarada Ganti, CISA, CISM, Allergan Pharma, USA

Mohamed Gohar, CISA, CISM, CRISC, CGEIT, CEH, CISSP, CLPTP,

COBIT 5, ISO 21500 LPM, ISO/IEC 20000 LI, ISO/IEC 24762 IT DRM,

ISO/IEC 27001 LA/LI, ISO/IEC 27005 LRM, ISO/IEC 27032 LCM,

ISO/IEC 27034 App Sec LI, ISO/IEC 38500 IT CGM, ITIL

Practitioner/Expert, PMP, Resilia Practitioner, SSGB, TOGAF

Practitioner, Egypt

Shruti Shrikant Kulkarni, CISA, CRISC, CCSK, CISSP, ITIL V3 Expert, Interpublic Group, UK

S. Krishna Kumar, CISA, CISM, CGEIT, India

Vivian Mojuetan, CISA, CRISC, Vocalink, UK

Juan Carlos Morales, CISA, CISM, CGEIT, CRISC, Guatemala

Mukesh Nathani, CISA, PMP, Deloitte, Canada

Dapo Ogunkola, CISA, CRISC, ACA, CFE, CFSA, EY, UK

Ganiyu Oladimeji, CISA, CISM, CRISC, Moshood Abiola Polytechnic, Nigeria

Opeyemi Onifade, CISA, CISM, CGEIT, BRMP, CCSP, CISSP, ISO

27001LA, PCI-QSA, Afenoid Enterprise Limited, Nigeria

Teju Oyewole, CISA, CISM, CRISC, CCSP, CISSP, PMP, Indigo Books &

Music, Canada

Vaibhav Patkar, CISA, CISM, CGEIT, CRISC, CISSP, India

Esteban Pizzini, CISA, Argentina

Robert Prince, CISA, CISSP, Sempra Energy, USA

Shahid Qureshi, CISA, CGA, CIA (USA), CPA, FCCA (UK), FCMA, FCIS, FCSM, Canada

Sreekrishna Rao, CISA, UK

Salah Riahi, CISA, CGEIT, CIA, CPA, Audit Risk Consulting, Tunisia Anamika Roy, CISA, CA, CIA, SFC, BDO USA LLP, USA

Markus Schiemer, CISA, CGEIT, CRISC, Microsoft, Austria

Xitij U. Shukla, Ph.D., CISA, Anand Agricultural University, India Vivek Silla, CISA, CISM, CRISC, CEH, CHFI, CICA, CIPM, CISSP, ISO

27001 Lead Auditor, ITIL Foundation, SCF, The Saudi Investment Bank, Saudi Arabia

Bhavani Suresh, CISA, CISM, CGEIT, COBIT Certified Assessor, Nbiz Infosol, UAE

Katalin Szenes, CISA, CISM, CGEIT, CISSP, Obuda University, Hungary Vikrant V. Tanksale, CISA, Oman

Luong Trung Thanh, CISA, CISM, CGEIT, Vietnam

Ross E. Wescott, CISA, CCP, CIA (ret.), CUERME, Wescott and Associates, USA

Prometheus Yang, CISA, CISM, CRISC, Taiwan

ISACA has begun planning the next edition of the *CISA® Review Manual*.

Volunteer participation drives the success of the manual. If you are interested in becoming a member of the select group of professionals involved in this global project, please visit *engage.isaca.org.*

Previous CISA Job Practice	New CISA Job Practice
Domain 1: The Process of Auditing Information Systems (21%) Domain 2: Governance and Management of IT (16%) Domain 3: Information Systems Acquisition, Development and Implementation (18%) Domain 4: Information Systems Operations, Maintenance and Service Management (20%) Domain 5: Protection of Information Assets (25%)	Domain 1: Information System Auditing Process (21%) Domain 2: Governance and Management of IT (17%) Domain 3: Information Systems Acquisition, Development and Implementation (12%) Domain 4: Information Systems Operations and Business Resilience (23%) Domain 5: Protection of Information Assets (27%)

New—CISA Job Practice

Beginning in 2019, the Certified Information Systems Auditor (CISA) exam tests the new CISA job practice.

An international job practice analysis is conducted periodically to maintain the validity of the CISA certification program. A new job practice forms the basis of the CISA.

The primary focus of the job practice is on the current tasks performed and the knowledge used by CISAs. By gathering evidence of the current work practice of CISAs, ISACA ensures that the CISA program continues to meet the high standards for the certification of professionals throughout the world.

The findings of the CISA job practice analysis are carefully considered and directly influence the development of new test specifications to ensure that the CISA exam reflects the most current best practices.

The new job practice reflects the areas of study to be tested and is compared below to the previous job practice. The complete CISA job practice is available at *www.isaca.org/cisajobpractice*.

Table of Contents

About This Manual

Overview

Format of This Manual

Preparing for the CISA Exam

Getting Started

Using the CISA Review Manual

Manual Features

Using the CISA Review Manual and Other ISACA Resources

About the CISA Review Questions, Answers and Explanations

Products

Chapter 1:

Information System Auditing Process

Overview

Domain 1 Exam Content Outline

Learning Objectives/Task Statements

Suggested Resources for Further Study

Self-assessment Questions

Answers to Self-assessment Questions

Part A: Planning

1.0 Introduction

1.1 IS Audit Standards, Guidelines and Codes of Ethics

1.1.1 ISACA IS Audit and Assurance Standards

1.1.2 ISACA IS Audit and Assurance Guidelines

1.1.3 ISACA Code of Professional Ethics

1.1.4 ITAF™

1.2 Business Processes

1.2.1 IS Internal Audit Function

Audit Charter

1.2.2 Management of the IS Audit Function

IS Audit Resource Management

1.2.3 Audit Planning

Individual Audit Assignments

1.2.4 Effect of Laws and Regulations on IS Audit Planning

1.2.5 Business Process Applications and Controls

Ecommerce

Electronic Data Interchange

Email

Point-of-sale Systems

Electronic Banking

Electronic Funds Transfer

Automated Teller Machine

Electronic Finance

Integrated Manufacturing Systems

Interactive Voice Response

Purchase Accounting System

Image Processing

Industrial Control Systems

Artificial Intelligence and Expert Systems

Supply Chain Management

Customer Relationship Management

1.2.6 Using the Services of Other Auditors and Experts

1.3 Types of Controls

1.3.1 Control Objectives and Control Measures

IS Control Objectives

1.3.2 Evaluation of the Control Environment

1.3.3 General Controls

1.3.4 IS-specific Controls

1.4 Risk-based Audit Planning

1.4.1 Audit Risk and Materiality

1.4.2 Risk Assessment

1.4.3 IS Audit Risk Assessment Techniques

1.4.4 Risk Analysis

1.5 Types of Audits and Assessments

Part B: Execution

1.6 Audit Project Management

1.6.1 Audit Objectives

1.6.2 Audit Phases

1.6.3 Audit Programs

Minimum Skills to Develop an Audit Program

1.6.4 Audit Work Papers

1.6.5 Fraud, Irregularities and Illegal Acts

1.7 Sampling Methodology

1.7.1 Compliance Versus Substantive Testing

1.7.2 Sampling

Sampling Risk

1.8 Audit Evidence Collection Techniques

1.8.1 Interviewing and Observing Personnel in Performance of Their Duties

1.9 Data Analytics

1.9.1 Computer-assisted Audit Techniques

CAATs as a Continuous Online Audit Approach

1.9.2 Continuous Auditing and Monitoring

1.9.3 Continuous Auditing Techniques

1.10 Reporting and Communication Techniques

1.10.1 Communicating Audit Results

1.10.2 Audit Report Objectives

1.10.3 Audit Report Structure and Contents

1.10.4 Audit Documentation

1.10.5 Follow-up Activities

1.10.6 Types of IS Audit Reports

1.11 Quality Assurance and Improvement of the Audit Process

1.11.1 Control Self-assessment

Objectives of CSA

Benefits of CSA

Disadvantages of CSA

The IS Auditor’s Role in CSA

1.11.2 Integrated Auditing

Case Study

Answers to Case Study Questions

Chapter 2:

Governance and Management of IT

Overview

Domain 2 Exam Content Outline

Learning Objectives/Task Statements

Suggested Resources for Further Study

Self-assessment Questions

Answers to Self-assessment Questions

Part A: IT Governance

2.0 Introduction

2.1 IT Governance and IT Strategy

2.1.1 Enterprise Governance of Information and Technology

2.1.2 Good Practices for EGIT

2.1.3 Audit’s Role in EGIT

2.1.4 Information Security Governance

Effective Information Security Governance

2.1.5 Information Systems Strategy

2.1.6 Strategic Planning

2.1.7 Business Intelligence

Data Governance

2.2 IT-related Frameworks

2.3 IT Standards, Policies and Procedures

2.3.1 Standards

2.3.2 Policies

Information Security Policy

Review of the Information Security Policy

2.3.3 Procedures

2.3.4 Guidelines

2.4 Organizational Structure

2.4.1 IT Governing Committees

2.4.2 Roles and Responsibilities of Senior Management and Boards of Directors

Board of Directors

Senior Management

Information Security Standards Committee

Chief Information Security Officer

IT Steering Committee

Matrix of Outcomes and Responsibilities

2.4.3 IT Organizational Structure and Responsibilities

IT Roles and Responsibilities

2.4.4 Segregation of Duties Within IT

Segregation-of-duties Controls

2.4.5 Auditing IT Governance Structure and Implementation

Reviewing Documentation

2.5 Enterprise Architecture

2.6 Enterprise Risk Management

2.6.1 Developing a Risk Management Program

2.6.2 Risk Management Process

Step 1: Asset Identification

Step 2: Evaluation of Threats and Vulnerabilities to Assets

Step 3: Evaluation of the Impact

Step 4: Calculation of Risk

Step 5: Evaluation of and Response to Risk

2.6.3 Risk Analysis Methods

Qualitative Analysis Methods

Semiquantitative Analysis Methods

Quantitative Analysis Methods

2.7 Maturity Models

2.7.1 Capability Maturity Model Integration

2.7.2 Initiating, Diagnosing, Establishing, Acting and Learning

(IDEAL) Model

2.8 Laws, Regulations and Industry Standards Affecting the Organization

2.8.1 Governance, Risk and Compliance

2.8.2 Impact of Laws, Regulations and Industry Standards on IS Audit

Part B: IT Management

2.9 IT Resource Management

2.9.1 Value of IT

2.9.2 Implementing IT Portfolio Management

IT Portfolio Management Versus Balanced Scorecard

2.9.3 IT Management Practices

2.9.4 Human Resource Management

Hiring

Employee Handbook

Promotion Policies

Training

Scheduling and Time Reporting

Terms and Conditions of Employment

During Employment

Employee Performance Evaluations

Required Vacations

Termination Policies

2.9.5 Organizational Change Management

2.9.6 Financial Management Practices

IS Budgets

Software Development

2.9.7 Information Security Management

2.10 IT Service Provider Acquisition and Management

2.10.1 Outsourcing Practices and Strategies

Industry Standards/Benchmarking

Globalization Practices and Strategies

2.10.2 Outsourcing and Third-party Audit Reports

2.10.3 Cloud Governance

2.10.4 Governance in Outsourcing

2.10.5 Capacity and Growth Planning

2.10.6 Third-party Service Delivery Management

2.10.7 Monitoring and Review of Third-party Services

2.10.8 Managing Changes to Third-party Services

Service Improvement and User Satisfaction

2.11 IT Performance Monitoring and Reporting

2.11.1 Performance Optimization

Critical Success Factors

Methodologies and Tools

2.11.2 Tools and Techniques

IT Balanced Scorecard

2.12 Quality Assurance and Quality Management of IT

2.12.1 Quality Assurance

2.12.2 Quality Management

Case Study

Answers to Case Study Questions

Chapter 3:

Information Systems Acquisition, Development and

Implementation

Overview

Domain 3 Exam Content Outline

Learning Objectives/Task Statements

Suggested Resources for Further Study

Self-assessment Questions

Answers to Self-assessment Questions

Part A: Information Systems Acquisition and Development

3.0 Introduction

3.1 Project Governance and Management

3.1.1 Project Management Practices

3.1.2 Project Management Structure

3.1.3 Project Management Roles and Responsibilities

3.1.4 Project Management Techniques

3.1.5 Portfolio/Program Management

3.1.6 Project Management Office

Project Portfolio Database

3.1.7 Project Benefits Realization

3.1.8 Project Initiation

3.1.9 Project Objectives

3.1.10 Project Planning

Information System Development Project Cost Estimation

Software Size Estimation

Function Point Analysis

Cost Budgets

Software Cost Estimation

Scheduling and Establishing the Time Frame

3.1.11 Project Execution

3.1.12 Project Controlling and Monitoring

Management of Scope Changes

Management of Resource Usage

Management of Risk

3.1.13 Project Closing

3.1.14 IS Auditor’s Role in Project Management

3.2 Business Case and Feasibility Analysis

3.2.1 IS Auditor’s Role in Business Case Development

3.3 System Development Methodologies

3.3.1 Business Application Development

3.3.2 SDLC Models

3.3.3 SDLC Phases

Phase 1—Feasibility Study

Phase 2—Requirements Definition

Phase 3A—Software Selection and Acquisition

Phase 3B—Design

Phase 4A—Configuration

Phase 4B—Development

Phase 5—Final Testing and Implementation

Phase 6—Post-implementation Review

3.3.4 IS Auditor’s Role in SDLC Project Management

3.3.5 Software Development Methods

Prototyping—Evolutionary Development

Rapid Application Development

Agile Development

Object-oriented System Development

Component-based Development

Web-Based Application Development

Software Reengineering

Reverse Engineering

DevOps

Business Process Reengineering and Process Change

3.3.6 System Development Tools and Productivity Aids

Computer-aided Software Engineering

Code Generators

Fourth-generation Languages

3.3.7 Infrastructure Development/Acquisition Practices

Project Phases of Physical Architecture Analysis

Planning Implementation of Infrastructure

3.3.8 Hardware/Software Acquisition

Acquisition Steps

IS Auditor’s Role in Hardware Acquisition

3.3.9 System Software Acquisition

Integrated Resource Management Systems

IS Auditor’s Role in Software Acquisition

3.4 Control Identification and Design

3.4.1 Input/Origination Controls

Input Authorization

Batch Controls and Balancing

Error Reporting and Handling

3.4.2 Processing Procedures and Controls

Data Validation and Editing Procedures

Processing Controls

Data File Control Procedures

3.4.3 Output Controls

3.4.4 Application Controls

IS Auditor’s Role in Reviewing Application Controls

3.4.5 User Procedures

3.4.6 Decision Support System

Design and Development

Implementation and Use

Risk Factors

Implementation Strategies

Assessment and Evaluation

DSS Common Characteristics

Part B: Information Systems Implementation

3.5 Testing Methodologies

3.5.1 Testing Classifications

Other Types of Testing

3.5.2 Software Testing

3.5.3 Data Integrity Testing

3.5.4 Application Systems Testing

Automated Application Testing

3.5.5 IS Auditor's Role in Information Systems Testing

3.6 Configuration and Release Management

3.7 System Migration, Infrastructure Deployment and Data Conversion

3.7.1 Data Migration

Refining the Migration Scenario

Fallback (Rollback) Scenario

3.7.2 Changeover (Go-Live or Cutover) Techniques

Parallel Changeover

Phased Changeover

Abrupt Changeover

3.7.3 System Implementation

Implementation Planning

3.7.4 System Change Procedures and the Program Migration Process Critical Success Factors

End-user Training

3.7.5 System Software Implementation

3.7.6 Certification/Accreditation

3.8 Post-implementation Review

3.8.1 IS Auditor's Role in Post-implementation Review

Case Study

Answers to Case Study Questions

Chapter 4:

Information Systems Operations and Business Resilience

Overview

Domain 4 Exam Content Outline

Learning Objectives/Task Statements

Suggested Resources for Further Study

Self-assessment Questions

Answers to Self-assessment Questions

Part A: Information Systems Operations

4.0 Introduction

4.1 Common Technology Components

4.1.1 Computer Hardware Components and Architectures

Input/Output Components

Types of Computers

4.1.2 Common Enterprise Back-end Devices

4.1.3 Universal Serial Bus

Risk Related to USBs

Security Controls Related to USBs

4.1.4 Radio Frequency Identification

Applications of RFID

Risk Associated With RFID

Security Controls for RFID

4.1.5 Hardware Maintenance Program

Hardware Monitoring Procedures

4.1.6 Hardware Reviews

4.2 IT Asset Management

4.3 Job Scheduling and Production Process Automation

4.3.1 Job Scheduling Software

4.3.2 Scheduling Reviews

4.4 System Interfaces

4.4.1 Risk Associated With System Interfaces

4.4.2 Security Issues in System Interfaces

4.4.3 Controls Associated With System Interfaces

4.5 End-user Computing

4.6 Data Governance

4.6.1 Data Management

Data Quality

Data Life Cycle

4.7 Systems Performance Management

4.7.1 IS Architecture and Software

4.7.2 Operating Systems

Software Control Features or Parameters

Software Integrity Issues

Activity Logging and Reporting Options

Operating System Reviews

4.7.3 Access Control Software

4.7.4 Data Communications Software

4.7.5 Utility Programs

4.7.6 Software Licensing Issues

4.7.7 Source Code Management

4.7.8 Capacity Management

4.8 Problem and Incident Management

4.8.1 Problem Management

4.8.2 Process of Incident Handling

4.8.3 Detection, Documentation, Control, Resolution and Reporting of Abnormal Conditions

4.8.4 Support/Help Desk

4.8.5 Network Management Tools

4.8.6 Problem Management Reporting Reviews

4.9 Change, Configuration, Release and Patch Management

4.9.1 Patch Management

4.9.2 Release Management

4.9.3 IS Operations

IS Operations Reviews

4.10 IT Service Level Management

4.10.1 Service Level Agreements

4.10.2 Monitoring of Service Levels

4.10.3 Service Levels and Enterprise Architecture

4.11 Database Management

4.11.1 DBMS Architecture

Detailed DBMS Metadata Architecture

Data Dictionary/Directory System

4.11.2 Database Structure

4.11.3 Database Controls

Object-oriented Database Management System.

4.11.4 Database Reviews

Part B: Business Resilience

4.12 Business Impact Analysis

4.12.1 Classification of Operations and Criticality Analysis

4.13 System Resiliency

4.13.1 Application Resiliency and Disaster Recovery Methods

4.13.2 Telecommunication Networks Resiliency and Disaster Recovery Methods

4.14 Data Backup, Storage and Restoration

4.14.1 Data Storage Resiliency and Disaster Recovery Methods

4.14.2 Backup and Restoration

Offsite Library Controls

Security and Control of Offsite Facilities

Media and Documentation Backup

Types of Backup Devices and Media

Periodic Backup Procedures

Frequency of Rotation

Types of Media and Documentation Rotated

4.14.3 Backup Schemes

Full Backup

Incremental Backup

Differential Backup

Method of Rotation

Record Keeping for Offsite Storage

4.15 Business Continuity Plan

4.15.1 IT Business Continuity Planning

4.15.2 Disasters and Other Disruptive Events

Pandemic Planning

Dealing With Damage to Image, Reputation or Brand

Unanticipated/Unforeseeable Events

4.15.3 Business Continuity Planning Process

4.15.4 Business Continuity Policy

4.15.5 Business Continuity Planning Incident Management

4.15.6 Development of Business Continuity Plans

4.15.7 Other Issues in Plan Development

4.15.8 Components of a Business Continuity Plan

Key Decision-making Personnel

Backup of Required Supplies

Insurance

4.15.9 Plan Testing

Specifications

Test Execution

Documentation of Results

Results Analysis

Plan Maintenance

Business Continuity Management Good Practices

4.15.10 Summary of Business Continuity

4.15.11 Auditing Business Continuity

Reviewing the Business Continuity Plan

Evaluation of Prior Test Results

Evaluation of Offsite Storage

Evaluation of Security at the Offsite Facility

Interviewing Key Personnel

Reviewing the Alternative Processing Contract

Reviewing Insurance Coverage

4.16 Disaster Recovery Plans

4.16.1 Recovery Point Objective and Recovery Time Objective

4.16.2 Recovery Strategies

4.16.3 Recovery Alternatives

Contractual Provisions

Procuring Alternative Hardware

4.16.4 Development of Disaster Recovery Plans

IT DRP Contents

IT DRP Scenarios

Recovery Procedures

Organization and Assignment of Responsibilities

4.16.5 Disaster Recovery Testing Methods

Types of Tests

Testing

Test Results

4.16.6 Invoking Disaster Recovery Plans

Case Study

Answers to Case Study Questions

Chapter 5:

Protection of Information Assets

Overview

Domain 5 Exam Content Outline

Learning Objectives/Task Statements

Suggested Resources for Further Study

Self-assessment Questions

Answers to Self-Assessment Questions

Part A: Information Asset Security and Control

5.0 Introduction

5.1 Information Asset Security Frameworks, Standards and Guidelines

5.1.1 Auditing the Information Security Management Framework

Reviewing Written Policies, Procedures and Standards

Formal Security Awareness and Training

Data Ownership

Data Owners

Data Custodians

Security Administrator

New IT Users

Data Users

Documented Authorizations

Terminated Employee Access

Security Baselines

Access Standards

5.2 Privacy Principles

5.2.1 Audit Considerations for Privacy

5.3 Physical Access and Environmental Controls

5.3.1 Managerial, Technical and Physical Controls

5.3.2 Control Monitoring and Effectiveness

5.3.3 Environmental Exposures and Controls

Equipment Issues and Exposures Related to the Environment

Controls for Environmental Exposures

5.3.4 Physical Access Exposures and Controls

Physical Access Issues and Exposures

Physical Access Controls

Auditing Physical Access

5.4 Identity and Access Management

5.4.1 System Access Permission

5.4.2 Mandatory and Discretionary Access Controls

5.4.3 Information Security and External Parties

Identification of Risk Related to External Parties

Addressing Security When Dealing With Customers

Human Resources Security and Third Parties

5.4.4 Logical Access

Logical Access Exposures

Familiarization With the Enterprise’s IT Environment

Paths of Logical Access

5.4.5 Access Control Software

5.4.6 Identification and Authentication

5.4.7 Logon IDs and Passwords

Features of Passwords

Login ID and Password Good Practices

Token Devices, One-time Passwords

5.4.8 Biometrics

Physically Oriented Biometrics

Behavior-oriented Biometrics

Management of Biometrics

5.4.9 Single Sign-on

5.4.10 Authorization Issues

Access Control Lists

Logical Access Security Administration

Remote Access Security

5.4.11 Audit Logging in Monitoring System Access

Access Rights to System Logs

Tools for Audit Trail (Logs) Analysis

Cost Considerations

5.4.12 Naming Conventions for Logical Access Controls

5.4.13 Federated Identity Management

5.4.14 Auditing Logical Access

Familiarization With the IT Environment

Assessing and Documenting the Access Paths

Interviewing Systems Personnel

Reviewing Reports From Access Control Software

Reviewing Application Systems Operations Manual

5.4.15 Data Leakage

Data Leak Prevention

5.5 Network and End-point Security

5.5.1 IS Network Infrastructure

5.5.2 Enterprise Network Architectures

5.5.3 Types of Networks

5.5.4 Network Services

5.5.5 Network Standards and Protocols

5.5.6 OSI Architecture

5.5.7 Application of the OSI Model in Network Architectures

Local Area Network

Wide Area Network

Virtual Private Networks

TCP/IP and Its Relation to the OSI Reference Model

Network Administration and Control

Network Performance Metrics

Applications in a Networked Environment

On-demand Computing

5.5.8 Network Infrastructure Security

Client-server Security

Internet Security Controls

Firewall Security Systems

Development and Authorization of Network Changes

5.5.9 Shadow IT

5.6 Data Classification

5.7 Data Encryption and Encryption-related Techniques

5.7.1 Key Elements of Encryption Systems

5.7.2 Symmetric Key Cryptographic Systems

5.7.3 Public (Asymmetric) Key Cryptographic Systems

Quantum Cryptography

Digital Signatures

Digital Envelope

5.7.4 Applications of Cryptographic Systems

Transport Layer Security

IP Security

Secure Shell

Secure Multipurpose Internet Mail Extensions (S/MIME)

5.8 Public Key Infrastructure

5.9 Web-based Communication Technologies

5.9.1 Voice-over IP

VoIP Security Issues

5.9.2 Private Branch Exchange

PBX Risk

PBX Audit

5.9.3 Email Security Issues

5.9.4 Peer-to-peer Computing

5.9.5 Instant Messaging

5.9.6 Social Media

5.9.7 Cloud Computing

5.10 Virtualized Environments

5.10.1 Key Risk Areas

5.10.2 Typical Controls

5.11 Mobile, Wireless and Internet-of-things Devices

5.11.1 Mobile Computing

Bring Your Own Device

Internet Access on Mobile Devices

5.11.2 Wireless Networks

Wireless Wide Area Networks

Wireless Local Area Networks

WEP and Wi-fi Protected Access (WPA/WPA2)

Wireless Personal Area Networks

Ad Hoc Networks

Public Global Internet Infrastructure

Wireless Security Threats and Risk Mitigation

5.11.3 Internet of Things

Part B: Security Event Management

5.12 Security Awareness Training and Programs

5.13 Information System Attack Methods and Techniques

5.13.1 Fraud Risk Factors

5.13.2 Computer Crime Issues and Exposures

5.13.3 Internet Threats and Security

Network Security Threats

Passive Attacks

Active Attacks

Causal Factors for Internet Attacks

5.13.4 Malware

Virus and Worm Controls

Management Procedural Controls

Technical Controls

Anti-malware Software Implementation Strategies

Targeted Attacks

5.14 Security Testing Tools and Techniques

5.14.1 Testing Techniques for Common Security Controls

Terminal Cards and Keys

Terminal Identification

Logon IDs and Passwords

Controls Over Production Resources

Logging and Reporting of Computer Access Violations

Bypassing Security and Compensating Controls

5.14.2 Network Penetration Tests

5.14.3 Threat Intelligence

5.15 Security Monitoring Tools tand Techniques

5.15.1 Intrusion Detection Systems

Features

Limitations

Policy

5.15.2 Intrusion Prevention Systems

Honeypots and Honeynets

Full Network Assessment Reviews

5.15.3 Security Information and Event Management

5.16 Incident Response Management

5.17 Evidence Collection and Forensics

5.17.1 Computer Forensics

Data Protection

Data Acquisition

Imaging

Extraction

Interrogation

Ingestion/Normalization

Reporting

5.17.2 Protection of Evidence and Chain of Custody

Case Study

Answer to Case Study Questions

Appendix A: CISA Exam General Information

Appendix B: CISA 2019 Job Practice

Glossary

Acronyms

Index

Domain 1	Information System Auditing Process	21 percent
Domain 2	Governance and Management of IT	17 percent
Domain 3	Information Systems Acquisition, Development, and Implementation	12 percent
Domain 4	Information Systems Operations and Business Resilience	23 percent
Domain 5	Protection of Information Assets	27 percent

About This Manual

OVERVIEW

The *CISA® Review Manual 27th Edition* is intended to assist candidates with preparing for the CISA exam. This manual is one source of preparation for the exam and is not the only source. **It is not a comprehensive collection of all the information and experience that are required to pass the exam.**

No single publication offers such coverage and detail. If candidates read through the manual and encounter a topic that is new to them or one in which they feel their knowledge and experience are limited, they should seek additional

references. The CISA exam is a combination of questions that test candidates' technical and practical knowledge, and their ability to apply their experienced-based knowledge in given situations.

The *CISA® Review Manual 27th Edition* provides the knowledge and activities for the functions in the CISA job practice content areas and as described in the *ISACA Exam Candidate Information Guide*

(www.isaca.org/examguide): **Note:** Each chapter reviews the knowledge that CISA candidates are expected to understand to support and accomplish the tasks that they should be able to accomplish for a job practice domain. These tasks

constitute the current practices for the IS auditor. The detailed CISA job practice can be viewed at *www.isaca.org/cisajobpractice.* The CISA exam is based on this job practice.

The manual has been developed and organized to assist candidates in their study. CISA candidates should evaluate their strengths, based on knowledge and experience, in each of these areas.

FORMAT OF THIS MANUAL

Each *CISA Review Manual* chapter follows the same format:

• The overview section provides a summary of the focus of the chapter, along with:

– The domain exam content outline

– Related task statements

– Suggested resources for further study

– Self-assessment questions

• The content section includes:

– Content to support the different areas of the exam content outline

– Definition of terms commonly found on the exam

– Case studies to reinforce learning of each domain

Material included is pertinent for CISA candidates' knowledge and/or understanding when preparing for the CISA certification exam.

The structure of the content includes numbering to identify the chapter where a topic is located and the headings of the subsequent levels of topics addressed in the chapter (e.g., 2.6.3 Risk Analysis Methods, is a subtopic of Enterprise Risk Management in chapter 2). Relevant content in a subtopic is bolded for specific attention.

Understanding the material in this manual is one measurement of a candidate's knowledge, strengths and weaknesses, and an indication of areas where additional or focused study is needed. However, written material is not a substitute for experience. **CISA exam questions will test the candidate's practical application of this knowledge.**

Although every effort is made to address the majority of information that candidates are expected to know, not all examination questions are necessarily covered in the manual, and candidates will need to rely on professional experience to provide the best answer.

Throughout the manual, the word "association" refers to ISACA. Also, please note that the manual has been written using standard American English.

Note: The *CISA® Review Manual 27th Edition* is a living document. As technology advances, the manual will be updated to reflect such advances.

Further updates to this document before the date of the exam may be viewed at *www.isaca.org/studyaidupdates.*

PREPARING FOR THE CISA EXAM

The CISA exam evaluates a candidate's practical knowledge, including experience and application, of the job practice domains as described in this review manual. ISACA recommends that the exam candidate look to multiple resources to prepare for the exam, including this manual, the *CISA®*

Questions, Answers & Explanation Manual 12th Edition or database, and external publications. This section will cover some tips for studying for the exam

and how best to use this manual in conjunction with other resources.

GETTING STARTED

Having adequate time to prepare for the CISA exam is critical. Most candidates spend between three and six months studying prior to taking the exam. Make sure you set aside a designated time each week to study, which you may wish to increase as your exam date approaches.

Developing a plan for your study efforts can also help you make the most effective use of your time prior to taking the exam.

CISA Self-Assessment

In order to study effectively for the CISA exam, you should first identify the job practice areas in which you are weak. A good starting point is the CISA

self-assessment, available at *https://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Prepare-for-the-Exam/Pages/CISA-Self-Assessment.aspx.*

This 50-question sample exam is based on the question distribution of the CISA exam and can provide you with a high-level evaluation of your areas of need. When you complete the self-assessment, you will receive a summary of how you performed in each of the five job practice domains. You can use this summary to review the task and knowledge statements in the job practice and get an idea of where you should primarily focus your study efforts.

USING THE CISA REVIEW MANUAL

The *CISA Review Manual* is divided into five chapters, each corresponding with a domain in the CISA Job Practice. While the manual does not include every concept that could be tested on the CISA exam, it does cover a breadth of knowledge that provides a solid base for the exam candidate. The manual is one source of preparation for the exam and should not be thought of as the only source nor viewed as a comprehensive collection of all the information and experience required to pass the exam.

MANUAL FEATURES

The *CISA Review Manual* includes several features to help you navigate the CISA job practice and enhance your learning and retention of the material.

Overview

The overview provides the context of the domain, including the exam content outline areas and applicable learning objectives/task statements.

Suggested Resources for Further Study

As many of the concepts presented within the review manual are complex, you may find it useful to refer to external sources to supplement your understanding of these concepts. The suggested resources are references you can use to help to enhance your study efforts as they relate to each chapter.

Self-assessment Questions and Answers

The self-assessment questions at the end of section one of each chapter assist

in understanding how a CISA question could be presented on the CISA exam and should not be used independently as a source of knowledge. Self-assessment questions should not be considered a measurement of the candidate's ability to answer questions correctly on the CISA exam for that area. The questions are intended to familiarize the candidate with question structure and may or may not be similar to questions that will appear on the actual examination.

Case Studies

Case studies provide scenario-based learning that focuses on the concepts presented within each chapter. Each case study includes an IS audit scenario related to each domain and questions related to the scenario. The purpose of these case studies is to provide a real-world perspective on the content of each domain and how it relates to the CISA's practice.

Glossary

A glossary is included at the end of the manual and contains terms that apply to the material included in the chapters. Also included are terms that apply to

related areas not specifically discussed. The glossary is an extension of the text in the manual and can, therefore, be another indication of areas in which the candidate may need to seek additional references.

USING THE CISA REVIEW MANUAL AND OTHER ISACA RESOURCES

The CISA Review Manual can be used in conjunction with other CISA exam preparation activities. The following products are based on the CISA job practice, and referenced task and knowledge statements can be used to find related content within the *CISA Review Manual*. These resources include:

• *CISA Review Questions, Answers & Explanations Manual 12th Edition*

• CISA Review Questions, Answers & Explanations Database—12 Month Subscription

• CISA Online Review Course

• CISA review courses (provided by local ISACA chapters and accredited training organizations)

ABOUT THE CISA REVIEW QUESTIONS, ANSWERS AND EXPLANATIONS PRODUCTS

The *CISA Review Questions, Answers & Explanations Manual 12th Edition* consists of 1,000 multiple-choice study questions, answers and explanations arranged in the domains of the current CISA job practice.

Another study aid that is available is the CISA Review Questions, Answers &

Explanations Database—12 Month Subscription. The database consists of the 1,000 questions, answers and explanations included in the *CISA Review Questions, Answers & Explanations Manual 12th Edition*. With this product, CISA candidates can quickly identify their strengths and weaknesses by taking random sample exams of varying length and breaking the results down by domain. Sample exams also can be chosen by domain, allowing for concentrated study, one domain at a time, and other sorting features such as the omission of

previously correctly answered questions are available.

Questions in these products are representative of the types of questions that could appear on the exam and include explanations of the correct and incorrect answers. Questions are sorted by the CISA domains and as a sample test. These products are ideal for use in conjunction with the *CISA Review Manual 27th Edition*. They can be used as study sources throughout the study process or as part of a final review to determine where candidates may need additional study. It should be noted that these questions and suggested answers are provided as examples; they are not actual questions from the examination and may differ in content from those that actually appear on the exam.

Types of Questions on the CISA Exam

CISA exam questions are developed with the intent of measuring and testing practical knowledge and the application of IS audit/assurance principles and standards. As previously mentioned, all questions are presented in a multiple-choice format and are designed for one best answer.

Read each question carefully. Knowing that these types of questions are asked and how to study to answer them will go a long way toward answering them correctly. The best answer is of the choices provided. There can be many potential solutions to the scenarios posed in the questions, depending

on industry, geographical location, etc. Consider the information provided in the question and to determine the best answer of the options provided.

Each CISA question has a stem (question) and four options (answer choices).

The candidate is asked to choose the correct or best answer from the options.

The stem may be in the form of a question or incomplete statement. In some instances, a scenario or description also may be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided.

A helpful approach to these questions includes the following:

• Read the entire stem and determine what the question is asking. Look for key words such as “best,” “most,” and “first” and key terms that may indicate what

domain or concept is being tested.

• Read all of the options, and then read the stem again to see if you can eliminate any of the options based on your immediate understanding of the question.

• Reread the remaining options and bring in any personal experience you may have to determine which is the best answer to the question.

Another condition the candidate should consider when preparing for the exam is to recognize that IS audit is a global profession, and individual perceptions and experiences may not reflect the more global position or circumstance. Because the exam and CISA manuals are written for the international IS audit community, the candidate will be required to be somewhat flexible when reading a condition that may be contrary to the candidate's experience. It should be noted that CISA exam questions are written by experienced information systems audit professionals from around the world. Each question on the exam is reviewed by ISACA's CISA Exam Item Development Working Group, which consists of international members.

This geographic representation ensures that all exam questions are understood equally in every country and language.

Note: When using the CISA review materials to prepare for the exam, it should be noted that they cover a broad spectrum of information systems audit/assurance issues. Again, candidates should not assume that reading

these manuals and answering review questions will fully prepare them for the examination. Since actual exam questions often relate to practical experiences, candidates should refer to their own experiences and other reference sources and draw upon the experiences of colleagues and others who have earned the CISA designation.

Chapter 1:

Information System Auditing Process

Overview

Domain 1 Exam Content Outline

Learning Objectives/Task Statements

Suggested Resources for Further Study

Self-assessment Questions

Answers to Self-assessment Questions

Part A: Planning

1.0

Introduction

1.1

IS Audit Standards, Guidelines and Codes of Ethics

1.2

Business Processes

1.3

Types of Controls

1.4

Risk-based Audit Planning

1.5

Types of Audits and Assessments

Part B: Execution

1.6

Audit Project Management

1.7

Sampling Methodology

1.8

Audit Evidence Collection Techniques

1.9

Data Analytics

1.10 Reporting and Communication Techniques

1.11 Quality Assurance and Improvement of the Audit Process

Case Study

Case Study

Answers to Case Study Questions

OVERVIEW

The information systems (IS) auditing process encompasses the standards, principles, methods, guidelines, practices and techniques that an IS auditor uses to plan, execute, assess and review business or information systems and related processes. An IS auditor must have a thorough understanding of this auditing process as well as IS processes, business processes and controls designed to achieve organizational objectives and protect organizational assets.

This domain represents 21 percent of the CISA exam (approximately 32

questions).

DOMAIN 1 EXAM CONTENT OUTLINE

Part A: Planning

1. IS Audit Standards, Guidelines and Codes of Ethics

2. Business Processes

3. Types of Controls

4. Risk-based Audit Planning

5. Types of Audits and Assessments

Part B: Execution

1. Audit Project Management

2. Sampling Methodology

3. Audit Evidence Collection Techniques

4. Data Analytics

5. Reporting and Communication Techniques

6. Quality Assurance and Improvement of the Audit Process

LEARNING OBJECTIVES/TASK STATEMENTS

Within this domain, the IS auditor should be able to:

• Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization. (T1)

• Conduct an audit in accordance with IS audit standards and a risk-based IS

audit strategy. (T2)

• Communicate audit progress, findings, results and recommendations to stakeholders. (T3)

• Conduct audit follow-up to evaluate whether risk has been sufficiently addressed. (T4)

• Evaluate IT management and monitoring of controls. (T11)

• Utilize data analytics tools to streamline audit processes. (T36)

• Provide consulting services and guidance to the organization in order to improve the quality and control of information systems. (T37)

• Identify opportunities for process improvement in the organization's IT

policies and practices. (T38)

SUGGESTED RESOURCES FOR FURTHER STUDY

ISACA, Audit/Assurance programs, *www.isaca.org/auditprograms*

ISACA COBIT® Focus,

http://www.isaca.org/COBIT/focus/Pages/FocusHome.aspx

ISACA, *ITAFTM: A Professional Practices Framework for IS*

Audit/Assurance, *www.isaca.org/ITAF*

ISACA, *IT Audit Basics, www.isaca.org/Knowledge-Center/ITAFIS-*

Assurance-Audit-/IT-Audit-Basics/Pages/IT-Audit-Basics-Articles.aspx

ISACA, White papers, *www.isaca.org/whitepapers*

SELF-ASSESSMENT QUESTIONS

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided. Please note that these questions are not actual or retired exam items. Please see the section

"About This Manual" for more guidance regarding practice questions.

1-1

Which of the following outlines the overall authority to perform an IS

audit?

A. The audit scope with goals and objectives

B. A request from management to perform an audit

C. The approved audit charter

D. The approved audit schedule

1-2

In performing a risk-based audit, which risk assessment is completed **FIRST** by an IS auditor?

A. Detection risk assessment

B. Control risk assessment

C. Inherent risk assessment

D. Fraud risk assessment

1-3

Which of the following would an IS auditor **MOST** likely focus on when developing a risk-based audit program?

A. Business processes

B. Administrative controls

C. Environmental controls

D. Business strategies

1-4

Which of the following types of audit risk assumes an absence of compensating controls in the area being reviewed?

A. Control risk

B. Detection risk

C. Inherent risk

D. Sampling risk

1-5

An IS auditor performing a review of an application's controls finds a weakness in system software that could materially impact the

application. In this situation, an IS auditor should:

A. Disregard these control weaknesses because a system software

review is beyond the scope of this review.

B. Conduct a detailed system software review and report the control weaknesses.

C. Include in the report a statement that the audit was limited to a review of the application's controls.

D. Review the system software controls as relevant and recommend a detailed system software review.

1-6

Which of the following is the **MOST** important reason why an audit planning process should be reviewed at periodic intervals?

A. To plan for deployment of available audit resources

B. To consider changes to the risk environment

C. To provide inputs for documentation of the audit charter

D. To identify the applicable IS audit standards

1-7

Which of the following is **MOST** effective for implementing a control self-

assessment within small business units?

A. Informal peer reviews

B. Facilitated workshops

C. Process flow narratives

D. Data flow diagrams

1-8

Which of the following would an IS auditor perform **FIRST** when planning an IS audit?

A. Define audit deliverables.

B. Finalize the audit scope and audit objectives.

C. Gain an understanding of the business's objectives and purpose.

D. Develop the audit approach or audit strategy.

1-9

The approach an IS auditor should use to plan IS audit coverage should be based on:

A. risk.

B. materiality.

C. fraud monitoring.

D. sufficiency of audit evidence.

1-10 An organization performs a daily backup of critical data and software files and stores the backup tapes at an offsite location. The backup tapes are used to restore the files in case of a disruption. This is an example of a:

A. preventive control.

B. management control.

C. corrective control.

D. detective control.

ANSWERS TO SELF-ASSESSMENT QUESTIONS

1-1

A.

The audit scope is specific to a single audit and does not grant authority to perform an audit.

B.

A request from management to perform an audit is not sufficient

because it relates to a specific audit.

C.

The approved audit charter outlines the auditor's

responsibility, authority and accountability.

D.

The approved audit schedule does not grant authority to perform

an audit.

1-2

A.

Detection risk assessment is performed only after the inherent

and control risk assessments have been performed to determine

ability to detect errors within a targeted process.

B.

Control risk assessment is performed after the inherent risk

assessment has been completed and is to determine the level of

risk that remains after controls for the targeted process are in place.

C.

Inherent risk exists independently of an audit and can occur

because of the nature of the business. To successfully conduct an audit, it is important to be aware of the related business processes. To perform the audit, an IS auditor needs to

understand the business process; by understanding the

business process, an IS auditor better understands the

inherent risk.

D.

Fraud risk assessments are a subset of a control risk assessment in which an audit and assurance professional determines if the

control risk addresses the ability of internal and/or external

parties to commit fraudulent transactions within the system.

1-3

A.

A risk-based audit approach focuses on the understanding of

the nature of the business and being able to identify and

categorize risk. Business risk impacts the long-term viability of a specific business. Thus, an IS auditor using a risk-based audit approach must be able to understand business

processes.

B.

Administrative controls, while an important subset of controls,

are not the primary focus needed to understand the business

processes within scope of the audit.

C.

Like administrative controls, environmental controls are an

important control subset; however, they do not address high-level overarching business processes under review.

D.

Business strategies are the drivers for business processes;

however, in this case, an IS auditor is focusing on the business processes that were put in place to enable the organization to

meet the strategy.

A.

Control risk is the risk that a material error exists that will not be prevented or detected in a timely manner by the system of

internal controls.

B.

Detection risk is the risk that a material misstatement with a

management assertion will not be detected by an audit and

assurance professional’s substantive tests. It consists of two

components: sampling risk and nonsampling risk.

C.

Inherent risk is the risk level or exposure without considering the actions that management has taken or might take.

D.

Sampling risk is the risk that incorrect assumptions are made

about the characteristics of a population from which a sample is taken. Nonsampling risk is the detection risk not related to

sampling; it can be due to a variety of reasons, including, but not limited to, human error.

1-5

A.

An IS auditor is not expected to ignore control weaknesses just

because they are outside the scope of a current review.

B.

The conduct of a detailed systems software review may hamper

the audit’s schedule, and an IS auditor may not be technically

competent to do such a review at this time.

C.

If there are control weaknesses that have been discovered by an

IS auditor, they should be disclosed. By issuing a disclaimer, this responsibility would be waived.

D.

The appropriate option would be to review the systems

software as relevant to the review and recommend a detailed

systems software review for which additional resources may

be recommended.

1-6

A.

Planning for deployment of available audit resources is

determined by the audit assignments planned, which are

influenced by the planning process.

B.

Short- and long-term issues that drive audit planning can be

heavily impacted by changes to the risk environment,

technologies and business processes of the enterprise.

C.

The audit charter reflects the mandate of top management to the

audit function and resides at a more abstract level.

D.

Applicability of IS audit standards, guidelines and procedures is universal to any audit engagement and is not influenced by short-and long-term issues.

1-7

A.

Informal peer reviews would not be as effective because they

would not necessarily identify and assess all control issues.

B.

Facilitated workshops work well within small business units.

C.

Process flow narratives would not be as effective because they

would not necessarily identify and assess all control issues.

D.

Data flow diagrams would not be as effective because they would

not necessarily identify and assess all control issues.

1-8

A.

Defining audit deliverables is dependent upon having a thorough

understanding of the business's objectives and purpose.

B.

Finalizing the audit scope and objectives is dependent upon

having a thorough understanding of the business's objectives and purpose.

C.

The first step in audit planning is to gain an understanding of the business's mission, objectives and purpose—which, in

turn, identifies the relevant policies, standards, guidelines, procedures and organization structure.

D.

Developing the audit approach or strategy is dependent upon

having a thorough understanding of the business's objectives and purpose.

1-9

A.

Audit planning requires a risk-based approach.

B.

Materiality pertains to potential weaknesses or absences of

controls while planning a specific engagement, and whether such

weaknesses or absences of controls could result in a significant deficiency or a material weakness.

C.

Fraud monitoring pertains to the identification of fraud-related transactions and patterns and may play a part in audit planning, but only as it pertains to organizational risk.

D.

Sufficiency of audit evidence pertains to the evaluation of the

sufficiency of evidence obtained to support conclusions and

achieve specific engagement objectives.

1-10 A.

Preventive controls are those that avert problems before they

arise. Backup tapes cannot be used to prevent damage to files

and, therefore, cannot be classified as a preventive control.

B.

Management controls modify processing systems to minimize a

repeat occurrence of the problem. Backup tapes do not modify

processing systems and, therefore, do not fit the definition of a management control.

C.

A corrective control helps to correct or minimize the impact

of a problem. Backup tapes can be used for restoring the files in case of damage of files, thereby reducing the impact of a

disruption.

D.

Detective controls help to detect and report problems as they

occur. Backup tapes do not aid in detecting errors.

PART A: PLANNING

1.0 INTRODUCTION

Audits are conducted for a variety of reasons. An audit can help an organization ensure effective operations, affirm its compliance with various regulations and confirm that the business is functioning well and is prepared to meet potential challenges. An audit can also help to gain assurance on the level of protection available for information assets. Most significantly, an audit can assure stakeholders of the financial, operational and ethical well-being of the organization. IS audits support all those outcomes, with a special focus on the information and related systems upon which most businesses and public institutions depend for competitive advantage.

IS audit is the formal examination and/or testing of information systems to determine whether:

• Information systems are in compliance with applicable laws, regulations, contracts and/or industry guidelines.

• Information systems and related processes comply with governance criteria and related and relevant policies and procedures.

• IS data and information have appropriate levels of confidentiality, integrity and availability.

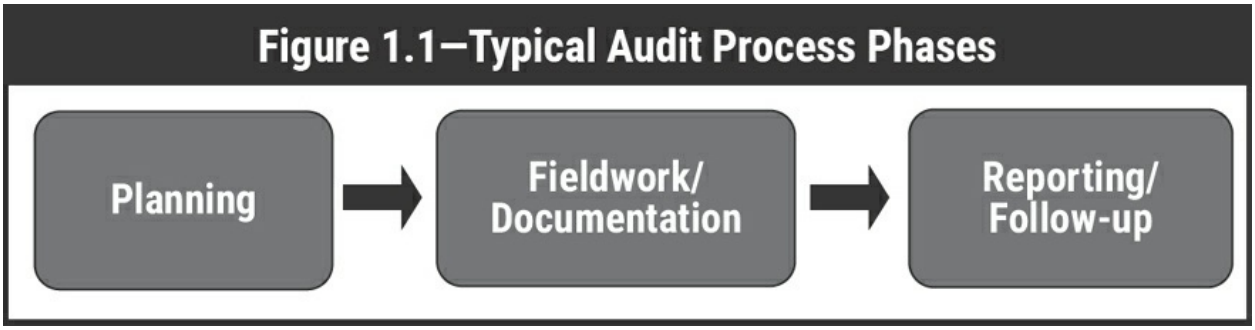
• IS operations are being accomplished efficiently and effectiveness targets are being met.

During the audit process, an IS auditor reviews the control framework, gathers evidence, evaluates the strengths and weaknesses of internal controls based on the evidence and prepares an audit report that presents weaknesses and recommendations for remediation in an objective manner to stakeholders.

In general terms, the typical audit process consists of three major phases

(figure 1.1):

• Planning



• Fieldwork/Documentation

• Reporting/Follow-up

Source: ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, USA, 2016

These main phases can be further broken down into subphases; for example, the reporting phase can be broken down into report writing and issuance, issue follow-up and audit closing. The organization and naming convention of these phases can be customized as long as the procedures and outcomes comply with applicable audit standards such as ITAF.

Note: Information systems are defined as the combination of strategic, managerial and operational activities and related processes involved in gathering, processing, storing, distributing and using information and its related technologies. Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components. IT is defined as the hardware, software, communication and other facilities used to input, store, process, transmit and output data in whatever form. Therefore, the terms “IS” and

“IT” will be used according to these definitions throughout the manual.

1.1 IS AUDIT STANDARDS, GUIDELINES AND CODES OF ETHICS

The credibility of any IS audit activity is largely determined by its adherence to commonly accepted standards. The fundamental elements of IS audit are defined

and provided within ISACA's IS audit and assurance standards and guidelines. ISACA's code of professional ethics guides the professional and

personal conduct of ISACA members and certification holders.

1.1.1 ISACA IS AUDIT AND ASSURANCE STANDARDS

ISACA IS Audit and Assurance Standards define mandatory requirements for IS auditing and reporting and inform a variety of audiences of critical information, such as the following:

• For IS auditors, the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics

• For management and other interested parties, the profession's expectations concerning the work of practitioners.

• For holders of the CISA designation, their professional performance requirements.

The framework for the ISACA IS Audit and Assurance Standards provides for multiple levels of documents:

• Standards define mandatory requirements for IS audit and assurance and reporting.

• Guidelines provide guidance in applying IS audit and assurance standards.

The IS auditor should consider them in determining how to achieve implementation of the above standards, use professional judgment in their application and be prepared to justify any departure from the standards.

• Tools and techniques provide examples of processes an IS auditor might follow in an audit engagement. The tools and techniques documents provide information on how to meet the standards when completing IS

auditing work, but do not set requirements.

ISACA IS Audit and Assurance Standards are divided into three categories—

general, performance and reporting:

• **General**—Provide the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with an IS auditor's ethics, independence, objectivity and due care as well as knowledge, competency and skill.

• **Performance**—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence,

and the exercising of professional judgment and due care

• **Reporting**—Address the types of reports, means of communication and the information communicated

1.1.2 ISACA IS AUDIT AND ASSURANCE GUIDELINES

ISACA IS Audit and Assurance Guidelines provide guidance and additional information on how to comply with the ISACA IS Audit and Assurance Standards. An IS auditor should do the following:

• Consider them in determining how to implement ISACA Audit and

Assurance Standards.

• Use professional judgment in applying them to specific audits.

• Be able to justify any departure from the ISACA Audit and Assurance Standards.

Note: The CISA candidate is not expected to know specific ISACA standard and guidance numbering or memorize any specific ISACA IS

audit and assurance standard or guideline. However, the exam will test a CISA candidate's ability to apply these standards and guidelines within the audit process. ISACA's IS Audit and Assurance Standards and

ISACA's IS Audit and Assurance Guidelines are living documents. The most current documents may be viewed at: *www.isaca.org/standards* and

www.isaca.org/guidelines .

1.1.3 ISACA CODE OF PROFESSIONAL ETHICS

ISACA's Code of Professional Ethics guides the professional and personal conduct of ISACA members and certification holders.

ISACA members and certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including audit, control, security and risk management.

2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.

3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.

4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority.

Such information shall not be used for personal benefit or released to inappropriate parties.

5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.

6. Inform appropriate parties of the results of work performed, including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.

7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise

information systems and technology, including audit, control, security and risk management.

Note: A CISA candidate is not expected to memorize the ISACA Code of

Professional Ethics *(www.isaca.org/certification/code-of-professional-*

ethics). The exam will test a candidate's understanding and application of the code.

1.1.4 ITAF™

ITAF is a comprehensive and good practice-setting reference model that does the following:

• Establishes standards that address IS auditor roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements

• Defines terms and concepts specific to IS assurance

• Provides guidance and tools and techniques on the planning, design, conduct and reporting of IS audit and assurance assignments

Note: A CISA candidate will not be tested on the organization or arrangement of the ITAF framework. However, the application of audit

and assurance standards is tested.

1.2 BUSINESS PROCESSES

An IS auditor must understand and be able to evaluate the business processes of the organization they are auditing. This includes a test and evaluation of the design and implementation of the operation of controls and the monitoring and testing of evidence to ensure that the internal controls within the business processes operate effectively.

A business process is an interrelated set of cross-functional activities or events that result in the delivery of a specific product or service to a customer. It is controlled by policies, procedures, practices and organizational structures designed to provide reasonable assurance that a business process will achieve its objectives. A business process owner is the individual responsible for identifying process requirements, approving process design and managing process performance, and should be at an appropriately high level in an organization to

have authority to commit resources to process-specific risk management activities.

1.2.1 IS INTERNAL AUDIT FUNCTION

The role of the IS internal audit function should be established by an audit charter approved by the board of directors and the audit committee (senior management, if these entities do not exist). Professionals should have a clear mandate to perform the IS audit function, which may be indicated in the audit charter.

Audit Charter

IS audit can be a part of internal audit, function as an independent group, or be integrated within a financial and operational audit to provide IT-related control assurance to the financial or management auditors. Therefore, the audit charter may include IS audit as an audit support function.

The charter should clearly state management's responsibility and objectives for, and delegation of authority to, the IS audit function. The highest level of management and the audit committee, if one exists, should approve this

charter. Once established, this charter should be changed only if the change can be and is thoroughly justified.

The responsibility, authority and accountability of the IS audit function should be appropriately documented in an audit charter or engagement letter.

An audit charter is an overarching document that covers the entire scope of audit activities in an entity while an engagement letter is more focused on a particular audit exercise that is sought to be initiated in an organization with a specific objective in mind. If IS audit services are provided by an external firm, the scope and objectives of these services should be documented in a formal contract or statement of work between the contracting organization and the service provider. In either case, the internal audit function should be independent and report to an audit committee, if one exists, or to the highest management level such as the board of directors.

Note: For additional guidance, see standard 1001 Audit Charter and guideline 2001 Audit Charter.

1.2.2 MANAGEMENT OF THE IS AUDIT FUNCTION

The IS audit function should be managed and led in a manner that ensures that the diverse tasks performed and achieved by the audit team will fulfill audit function objectives, while preserving audit independence and competence. Furthermore, managing the IS audit function should ensure value-added contributions to senior management in the efficient management of IT and achievement of business objectives.

Note: For additional guidance, see standards 1002 Organizational Independence, 1003 Professional Independence, 1004 Reasonable

Expectation and 1005 Due Professional Care, as well as the related guidelines: 2002, 2003, 2004 and 2005.

IS Audit Resource Management

IS technology is constantly changing. Therefore, it is important that IS

auditors maintain their competency through updates of existing skills and

obtain training directed toward new audit techniques and technological areas.

An IS auditor must be technically competent, having the skills and knowledge necessary to perform audit work. Further, an IS auditor must maintain technical competence through appropriate continuing professional education. Skills and knowledge should be taken into consideration when planning audits and assigning staff to specific audit assignments.

Preferably, a detailed staff training plan should be drawn up for the year based on the organization’s direction in terms of technology and related risk that needs to be addressed. This should be reviewed periodically to ensure that the training efforts and results are aligned to the direction that the audit organization is taking. Additionally, IS audit management should also provide the necessary IT resources to properly perform IS audits of a highly specialized nature (e.g., tools, methodology, work programs).

Note: For additional guidance, see standard 1006 Proficiency and guideline 2006 Proficiency.

1.2.3 AUDIT PLANNING

Audit planning is conducted at the beginning of the audit process to establish the overall audit strategy and detail the specific procedures to be carried out to implement the strategy and complete the audit. It includes both short- and long-term planning. Short-term planning considers audit issues that will be covered during the year, whereas long-term planning relates to audit plans that will consider risk-related issues regarding changes in the organization's IT strategic direction that will affect the organization's IT environment.

All of the relevant processes that represent the blueprint of the enterprise's business should be included in the audit universe. The audit universe ideally lists all of the processes that may be considered for audit. Each of these processes may undergo a qualitative or quantitative risk assessment by evaluating the risk in respect to defined, relevant risk factors. The risk factors are those factors that influence the frequency and/or business impact of risk scenarios. For example, for a retail business, reputation can be a critical risk factor. The evaluation of risk should ideally be based on inputs from the

business process owners. Evaluation of the risk factors should be based on objective criteria, although subjectivity cannot be completely avoided. For example, in respect to the reputation factor, the criteria (based on which inputs can be solicited from the business) may be rated as:

• **High**—A process issue may result in damage to the reputation of the organization that will take more than six months to recover.

• **Medium**—A process issue may result in damage to the reputation of the organization that will take less than six months but more than three months to recover.

• **Low**—A process issue may result in damage to the reputation of the organization that will take less than three months to recover.

In this example, the defined time frame represents the objective aspect of the criteria, and the subjective aspect of the criteria can be found in the business process owners' determination of the time frame—whether it is more than six months or less than three months. After the risk is evaluated for each relevant factor, an overall criterion may be defined to determine the overall risk of each of the processes.

The audit plan can then be constructed to include all of the processes that are rated “high,” which would represent the ideal annual audit plan. However, in practice, often the available resources are not sufficient to execute the entire ideal plan. This analysis will help the audit function to demonstrate to top management the gap in resourcing and give top management a good idea of the amount of risk that management is accepting if it does not add to or augment the existing audit resources.

Analysis of short- and long-term issues should occur at least annually. This is necessary to consider new control issues; changes in the risk environment, technologies and business processes; and enhanced evaluation techniques.

The results of this analysis for planning future audit activities should be reviewed by senior audit management and approved by the audit committee, if available, or alternatively by the board of directors and communicated to relevant levels of management. The annual planning should be updated if any key aspects of the risk environment have changed (e.g., acquisitions, new regulatory issues, market conditions).

Note: For additional guidance, see standards 1007 Assertions and 1008

Criteria and related guidelines 2007 and 2008.

Individual Audit Assignments

In addition to overall annual planning, each individual audit assignment must be adequately planned. An IS auditor should understand that other considerations, such as the results of periodic risk assessments, changes in the application of technology, and evolving privacy issues and regulatory requirements, may impact the overall approach to the audit. An IS auditor should also take into consideration system implementation/upgrade deadlines, current and future technologies, requirements from business process owners, and IS resource limitations.

When planning an audit, an IS auditor must understand the overall environment under review. This should include a general understanding of the various business practices and functions relating to the audit subject, as well as the types of information systems and technology supporting the activity. For example, an IS auditor should be familiar with the regulatory environment in which the business operates.

To perform audit planning, an IS auditor should perform the steps indicated in **figure 1.2**.

Figure 1.2—Steps to Perform Audit Planning

• Gain an understanding of the organization's mission, objectives, purpose and processes, which include information and processing requirements such as availability, integrity, security, and business technology and information confidentiality.

• Gain an understanding of the organization's governance structure and practices related to the audit objectives.

• Understand changes in the business environment of the auditee.

• Review prior work papers.

• Identify stated contents such as policies, standards and required guidelines, procedures, and organization structure.

• Perform a risk analysis to help in designing the audit plan.

• Set the audit scope and audit objectives.

• Develop the audit approach or audit strategy.

• Assign personnel resources to the audit.

• Address engagement logistics.

Note: For additional guidance, see standard 1201 Engagement Planning and guideline 2201 Engagement Planning.

1.2.4 EFFECT OF LAWS AND REGULATIONS ON IS AUDIT PLANNING

Each organization, regardless of its size or the industry within which it operates, will need to comply with a number of governmental and external requirements related to IS practices and controls and the manner in which data are used, stored and secured. Additionally, industry regulations can impact the way data are

processed, transmitted and stored (stock exchange, central banks, etc.). Special attention should be given to these issues in industries that are closely regulated.

Because of the dependency on information systems and related technology, several countries are making efforts to add legal regulations concerning IS

audit and assurance. The content of these legal regulations pertains to:

• Establishment of regulatory requirements

• Responsibilities assigned to corresponding entities

• Financial, operational and IS audit functions

Management at all levels should be aware of the external requirements relevant to the goals and plans of the organization, and to the responsibilities and activities of the information services department/function/activity.

There are two major areas of concern:

1. Legal requirements (i.e., laws, regulatory and contractual agreements) placed on audit or IS audit

2. Legal requirements placed on the auditee and its systems, data management, reporting, etc.

These areas impact the audit scope and audit objectives. The latter is important to internal and external audit and assurance professionals. Legal issues also impact the organization’s business operations in terms of compliance with ergonomic regulations.

An IS auditor would perform the following steps to determine an organization’s level of compliance with external requirements:

• Identify those government or other relevant external requirements dealing with:

– Electronic data, personal data, copyrights, ecommerce, esignatures, etc.

– Information system practices and controls

– The manner in which computers, programs and data are stored

– The organization or the activities of information technology services

– IS audits

• Document applicable laws and regulations.

• Assess whether the management of the organization and the IT function have considered the relevant external requirements in making plans and in setting policies, standards and procedures, as well as business application features.

• Review internal IT department/function/activity documents that address adherence to laws applicable to the industry.

• Determine adherence to established procedures that address these requirements.

• Determine if there are procedures in place to ensure contracts or agreements with external IT services providers reflect any legal requirements related to responsibilities.

Note: A CISA candidate will not be asked about any specific laws or regulations but may be questioned about how one would audit for

compliance with laws and regulations.

1.2.5 BUSINESS PROCESS APPLICATIONS AND

CONTROLS

In an integrated application environment, controls are embedded and designed into the business application that supports the processes. Business process control assurance involves evaluating controls at the process and activity levels. These controls may be a combination of management, programmed and manual controls. In addition to evaluating general controls that affect the processes, business process owner-specific controls—such as

establishing proper security and segregation of duties (SoD), periodic review and approval of access, and application controls within the business process

—are evaluated.

To effectively audit business application systems, an IS auditor must obtain a clear understanding of the application system under review.

Note: The content that follows includes examples of business application systems and architectures, related processes and risk. A CISA candidate should be familiar with these business application systems and

architectures, processes, risk and related controls, and IS audit implications and practices.

Numerous financial and operational functions are computerized for the purpose of improving efficiency and increasing the reliability of information.

These applications range from traditional (including general ledger, accounts payable and payroll) to industry-specific (such as bank loans, trade clearing and material requirements planning). Given their unique characteristics, computerized application systems add complexity to audit efforts. These characteristics may include limited audit trails, instantaneous updating and information overload. Application systems may reside in the various environments that follow.

Ecommerce

Ecommerce is the buying and selling of goods online. Typically, a buyer purchases goods and services from a website and provides delivery and payment details, including transfers or payment orders. The website may gather details about customers and offer other items that may be of interest.

The term ebusiness includes buying and selling online as well as customer support or relationships between businesses.

Ecommerce, as a general model, uses technology to enhance the processes of commercial transactions among a company, its customers and business partners. The technology used can include the Internet, multimedia, web browsers, proprietary networks, automatic teller machines (ATMs) and home

banking, and the traditional approach to electronic data interchange (EDI).

Ecommerce types include the following:

• **Business-to-business (B-to-B)**—Business conducted between organizations

• **Business-to-consumer (B-to-C)**—Business conducted between an organization and its customers

• **Consumer-to-consumer (C-to-C)**—Business conducted between customers, primarily using a third-party platform

• **Consumer-to-business (C-to-B)**—Business conducted between a consumer and a business. This is when consumers sell their products or services to a business.

• **Business-to-government (B-to-G)**—Business conducted between an organization and a public administration (e.g., government organizations) where the governmental organization promotes awareness and growth of ecommerce. In addition to public procurement, administrations may also offer the option of electronic interchange for such transactions as VAT

returns and the payment of corporate taxes.

• **Consumer-to-government (C-to-G)**—Business conducted between a consumer and a public administration or government. An example is electronic tax filing.

Typical ecommerce architectures include the following types:

• Single-tier architecture is a client-based application running on a single computer.

• Two-tier architecture is composed of the client and server.

• Three-tier architecture is comprised of the following:

– The presentation tier displays information that users can access directly such as a web page or an operating system’s (OS’s) graphical user interface.

– The application tier (business logic/applications) controls an application’s functionality by performing detailed processing.

– The data tier is usually comprised of the database servers, file shares, etc. and

the data access layer that encapsulates the persistence mechanisms and exposes the data.

The challenge of integrating diverse technologies within and beyond the business has increasingly led organizations to move to component-based systems that use a middleware infrastructure based around an application server. This supports current trends in the evolution of software development: building systems from quality and catalogued components, just as hardware is built. While this is yet to be fully realized, component models—notably Microsoft Component Object Model (COM) and Oracle Enterprise

JavaBeans—are widely used and fall under the grouping of “mobile code.”

Mobile code is software transferred between systems (i.e., transferred across a network) and executed on a local system using cross-platform code without explicit installation by the recipient computer (e.g., Adobe® Flash®, Shockwave®, Java applets, VBScripts, ActiveX). The continued adoption of mobile code brings another vector for the spread of malware via ever-evolving delivery vectors ranging from email to malicious websites and mobile device applications.

Ecomponents often seen in a B-to-C system include marketing, sales and customer service components (e.g., personalization, membership, product catalog, customer ordering, invoicing, shipping, inventory replacement, online training and problem notification). Application servers support a particular component model and provide services (such as data management, security and transaction management) either directly or through connection to another service or middleware product.

Application servers in conjunction with other middleware products provide for multitiered systems (a business transaction can span multiple platforms and software layers). For example, a system’s presentation layer typically will consist of a browser or other client application. A web server will be used to manage web content and connections, business logic and other services will be provided by the application server, and one or more database(s) will be used for data storage.

Databases play a key role in most ecommerce systems, maintaining data for website pages, accumulating customer information and storing click-stream data

for analyzing website usage. To provide full functionality and achieve back-end efficiencies, an ecommerce system may involve connections to in-

house legacy systems—accounting, inventory management or an enterprise resource planning (ERP) system—or business partner systems. Thus, further business logic and data persistence tiers are added.

For security reasons, persistent customer data should not be stored on web servers that are exposed directly to the Internet. Extensible Markup Language (XML) is also likely to form an important part of an organization's overall ecommerce architecture. While originally conceived as a technique to facilitate electronic publishing, XML was quickly used as a medium that could store and enclose any kind of structured information, so it could be passed between different computing systems. XML has emerged as a key means of exchanging a wide variety of data on the web and elsewhere. In addition to basic XML, a variety of associated standards has been and is continuing to be developed. Some of these include:

• **Extensible Stylesheet Language (XSL)**—Defines how an XML document is to be presented (e.g., on a web page)

• **XML query (XQuery)**—Deals with querying XML format data

• **XML encryption**—Deals with encrypting, decrypting and digitally signing XML documents

A particularly important offshoot of XML is web services. Web services represent a way of using XML format information to remotely invoke processing. Because a web services message can contain both an XML

document and a corresponding schema defining the document, in theory, it is self-describing and assists in achieving the goal of "loose coupling." If the format of a web services message changes, the receiving web services will still work, provided the accompanying schema is updated. This advantage, combined with the support for web services, means web services are now the key middleware to connect distributed web systems.

It is necessary to reach some agreement on metadata definitions for web services to serve as a means of enabling cooperative processing across organizational boundaries. Metadata are data about data, and the term is referred to in web

services' standards as ontology. Web services may be successfully called, and the resulting XML data may be successfully parsed by the calling program, but to use these data effectively it is necessary to

understand the business meaning of the data. This is similar to previous attempts at interorganizational computing (such as EDI), in which it was necessary to agree in advance on electronic document formats and meanings.

Ecommerce Risk

Ecommerce, as any other form of commerce, depends on the existence of a level of trust between two parties. For example, the Internet presents a challenge between the buyer and seller, similar to those a catalog or direct-mail retailer faces. The challenges are proving to buyers that the sellers are who they say they are and that their personal information, such as credit card numbers (and other personally identifiable information), will remain confidential; and that sellers cannot later refute the occurrence of a valid transaction. Some of the most important elements at risk are:

• **Confidentiality**—Potential consumers are concerned about providing unknown vendors with personal (sometimes sensitive) information for a number of reasons including the possible theft of credit card information from the vendor following a purchase. Connecting to the Internet via a browser requires running software on the computer that has been

developed by someone unknown to the organization. Moreover, the

medium of the Internet is a broadcast network, which means that whatever is placed on it is routed over wide-ranging and essentially uncontrolled paths. The current trend of outsourcing and hosting services on the cloud expands the risk perimeter beyond the boundaries of the transacting entity.

It is important to take into consideration the importance of security issues that extend beyond confidentiality objectives.

• **Integrity**—Data, both in transit and in storage, could be susceptible to unauthorized alteration or deletion (i.e., hacking or the ebusiness system itself could have design or configuration problems).

• **Availability**—The Internet allows customers to do business on a 24-hour,

seven-day-a-week basis. Hence, high availability is important, with any system's failure becoming immediately apparent to customers or business partners.

• **Authentication and nonrepudiation**—The parties to an electronic transaction should be in a known and trusted business relationship, which requires that they prove their respective identities before executing the transaction to prevent man-in-the-middle attacks (i.e., preventing the seller

from being an impostor). Then, after the fact, there must be some manner of ensuring that the transacting parties cannot deny that the transaction was completed and the terms on which it was completed.

• **Power shift to customers**—The Internet gives consumers unparalleled access to market information and generally makes it easier to shift between suppliers. Organizations participating in ebusiness need to make their offerings attractive and seamless in terms of service delivery. This will involve not only system design, but also reengineering of business processes. Back-end support processes need to be as efficient as possible because, in many cases, doing business over the Internet forces down prices (e.g., online share brokering). To avoid losing their competitive advantage of doing business online, organizations need to enhance their services, differentiate from the competition and build additional value. This explains the drive to personalize websites by targeting content based on analyzed customer behavior and allowing direct contact with staff through instant messaging technology and other means.

Ecommerce Requirements

Some ecommerce requirements include the following:

• Building a business case (IT as an enabler)

• Developing a clear business purpose

• Using technology to first improve costs

• Building a business case around the four C's: customers, costs, competitors and capabilities

Other requirements for ecommerce include:

• **Top-level commitment**—Because of the breadth of change required (i.e., business processes, company culture, technology and customer

boundaries), ecommerce cannot succeed without a clear vision and strong commitment from the top of an organization.

• **Business process reconfiguration**—Technology is not the key innovation needed to make ecommerce work, but it is the ingenuity needed to envision how that technology can enable the company to fundamentally reconfigure some of its basic business processes. This requires thinking that is outside-the-box and outside-the-walls (i.e., looking outside of the organization and understanding what customers are doing and how changes in the overall

process can create new value for them).

• **Links to legacy systems**—Organizations must take seriously the requirement to accelerate response times, provide real interaction to customers and customize responses to individual customers. Specifically, in applying enterprise application integration (EAI), organizations must create online interfaces and make sure those interfaces communicate with existing databases and systems for customer service and order processing.

A term often referred to in establishing this communication is

"middleware," which is defined as independent software and services that distributed business applications use to share computing resources across heterogeneous technologies. A range of middleware technologies—

message brokers, gateways, process managers, data transformation software and file transfer—are likely to be deployed to create an integration infrastructure. Increasingly, integration will be viewed not as a responsibility of an individual application development team, but as something to be managed across the organization using a standard approach and technologies.

IS Auditor's Role in the Ecommerce Business Process

An IS auditor should review the following:

• Interconnection agreements prepared prior to engaging in an ecommerce agreement. These agreements can be as simple as accepting terms of use to

detailed terms and conditions to be in place before the ecommerce interconnections are established.

• Security mechanisms and procedures that, taken together, constitute a security architecture for ecommerce (e.g., Internet firewalls, public key infrastructure [PKI], encryption, certificates, PCI DSS compliance and password management)

• Firewall mechanisms that are in place to mediate between the public network (the Internet) and an organization's private network

• A process whereby participants in an ecommerce transaction can be identified uniquely and positively (e.g., a process of using some combination of public and private key encryption and certifying key pairs)

• Procedures in place to control changes to an ecommerce presence

• Ecommerce application logs, which are monitored by responsible personnel. This includes OS logs and console messages, network

management messages, firewall logs and alerts, router management messages, intrusion detection alarms, application and server statistics, and system integrity checks.

• Methods and procedures to recognize security breaches when they occur (network and host-based intrusion detection systems [IDSs])

• Features in ecommerce applications to reconstruct the activity performed by the application

• Protections in place to ensure that data collected about individuals are not disclosed without the individuals' consent nor used for purposes other than that for which they are collected

• Means to ensure confidentiality of data communicated between customers and vendors (safeguarding resources such as through encrypted Secure Sockets Layer [SSL])

• Mechanisms to protect the presence of ecommerce and supporting private networks from computer viruses and to prevent them from propagating viruses to customers and vendors

• Features within the ecommerce architecture to keep all components from failing and allow them to repair themselves, if they should fail

• Plans and procedures to continue ecommerce activities in the event of an extended outage of required resources for normal processing

• Commonly understood practices and procedures to define management's intentions for the security of ecommerce

• Shared responsibilities within an organization for ecommerce security

• Communications from vendors to customers about the level of security in an ecommerce architecture

• Regular programs of audit and assessment of the security of ecommerce environments and applications to provide assurance that controls are present and effective

Electronic Data Interchange

EDI replaced the traditional paper document exchange, such as medical claims and records, purchase orders, invoices, or material release schedules.

Therefore, proper controls and edits need to be built within each organization's application system to allow this communication to take place.

General Requirements

An EDI system requires communications software, translation software and access to standards. Communications software moves data from one point to another, flags the start and end of an EDI transmission, and determines how acknowledgments are transmitted and reconciled. Translation software helps build a map and shows how the data fields from the application correspond to elements of an EDI standard. Later, it uses this map to convert data back and forth between the application and EDI formats.

To build a map, an EDI standard appropriate for the kind of EDI data to be transmitted is selected (e.g., specific standards for medical claims, patient records, invoices, purchase orders, advance shipping notices.). The final step is to write a partner profile that tells the system where to send each transaction and

how to handle errors and exceptions.

EDI system software includes transmission, translation and storage of transactions initiated by or destined for application processing. EDI is also an application system in that the functions it performs are based on business needs and activities. The applications, transactions and trading partners supported will change over time, and the intermixing of transactions, purchase orders, shipping notices, invoices and payments in the EDI process makes it necessary to include application processing procedures and controls in the EDI process.

In reviewing EDI, an IS auditor should be aware of the two approaches related to EDI: the traditional proprietary version of EDI used by large companies and government parties, and the development of EDI through the publicly available commercial infrastructure offered through the Internet. The difference between the approaches relates to cost, where use of a public commercial infrastructure such as the Internet provides significantly reduced costs versus development of a customized proprietary approach. From a security standpoint, risk associated with not having a completely trustworthy relationship arise in addressing Internet security and risk.

Traditional EDI

Moving data in a batch transmission process through the traditional EDI process generally involves three functions within each trading partner's

computer system:

1. **Communications handler**—Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public-switched network, multiple dedicated lines or a value-added network (VAN). VANs use computerized message switching and storage

capabilities to provide electronic mailbox services similar to a post office.

The VAN receives all the outbound transactions from an organization, sorts them by destination and passes them to recipients when they log on to check their mailbox and receive transmissions. They may also perform translation and verification services. VANs specializing in EDI

applications provide technical support, help desk and troubleshooting assistance

for EDI and telecommunications problems. VANs help in configuration of software, offer upgrades to telecommunications

connectivity, provide data and computer security, audit and trace transactions, recover lost data, and confirm service reliability and availability.

2. **EDI interface**—Interface function that manipulates and routes data between the application system and the communications handler. The interface consists of two components:

• EDI translator—This device translates the data between the standard format (ANSI X12) and a trading partner's proprietary format.

• Application interface—This interface moves electronic transactions to or from the application systems and performs data mapping. The EDI interface may generate and send functional acknowledgments, verify the identity of partners and check the validity of transactions by checking transmission information against a trading partner master file.

Functional acknowledgments are standard EDI transactions that tell the trading partners that their electronic documents were received and can act as an audit trail for EDI transactions.

3. **Application system**—The programs that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the controls for existing applications, if left unchanged, are usually unaffected.

Application-initiated transactions (such as purchase orders from the purchasing system) are passed to a common application interface for storage

and interpretation. All outbound transactions are formatted according to an externally defined standard and batched by destination and transaction type by the translator. The batches of transactions, like functional groups, are routed to the communications processor for transmission. This entire process is reversed for inbound transactions, including invoices destined for the purchasing and accounts payable systems. Controls need to recognize and deal with error conditions and provide feedback on the process for the EDI system to be considered well managed.

Web-based EDI

Web-based EDI has come into prominence because:

• Access through Internet service providers (ISPs) offers generic network access (i.e., not specific to EDI) for all connected computers, whereas VAN services have typically used a proprietary network or a network gateway linked with a specific set of proprietary networks. The result is a substantially reduced cost to EDI applications.

• It can attract new partners via web-based sites to exchange information, take orders, and link the website to back-end order processing and financial systems via EDI.

• New security products are available to address issues of confidentiality, authentication, data integrity, and nonrepudiation of origin and return.

• Improvements in the X12 EDI formatting standard web-based EDI trading techniques aim to improve the interchange of information between trading partners, suppliers and customers by bringing down the boundaries that restrict how they interact and do business with each other. For example, ISP service can provide functions similar to those of the more traditional VANs, but with a much broader array of available services (i.e., processing transactions of all types through the Internet). This is beneficial particularly for smaller organizations wanting to enter the ecommerce EDI market because ISPs have a ready network infrastructure of servers offering email, web services and the network of routers, and modems attached to a permanent, high-speed Internet “backbone” connection.

EDI Risk and Controls

The hybrid nature of EDI adds a new dimension to the design and audit of the EDI process. The traditional procedures for managed and controlled

implementation of system software—such as requirements definition, version and release identification, testing and limited implementation with a fallback strategy—apply to software used for EDI. In addition, there are issues and risk unique to EDI.

Transaction authorization is the biggest EDI risk. Because the interaction

between parties is electronic, no inherent authentication occurs.

Computerized data can look the same no matter what the source and do not include any distinguishing human element or signature.

Where responsibilities of trading partners are not clearly defined by a trading partner agreement, there could be uncertainty related to specific, legal liability. Therefore, it is important that, to protect both parties, any agreement is codified legally in what is known as a trading partner agreement. Another risk is the loss of business continuity. Corruption of EDI applications, whether done innocently or deliberately, could affect every EDI transaction undertaken by a company. This would have a negative impact on both customer and vendor relations. In an extreme situation, it could ultimately affect the ability of a company to stay in business.

Additional security types of risk include:

• Unauthorized access to electronic transactions

• Deletion or manipulation of transactions prior to or after establishment of application controls

• Loss or duplication of EDI transmissions

• Loss of confidentiality and improper distribution of EDI transactions while in the possession of third parties

EDI Process Controls

Security risk can be addressed by enforcing general controls and establishing an added layer of application control procedures over the EDI process that can take over where traditional application controls leave off. These controls need to secure the current EDI activity as well as historical activities that may be called on to substantiate business transactions should a dispute arise.

To protect EDI transmissions, the EDI process should include the following

electronic measures:

• Standards should be set to indicate that the message format and content are

valid to avoid transmission errors.

• Controls should be in place to ensure that standard transmissions are properly converted for the application software by the translation application.

• The receiving organization must have controls in place to test the reasonableness of messages received. This should be based on a trading partner's transaction history or documentation received that substantiates special situations.

• Controls should be established to guard against manipulation of data in active transactions, files and archives. Attempts to change records should be recorded by the system for management review and attention.

• Procedures should be established to determine messages are only from authorized parties and transmissions are properly authorized.

• Direct or dedicated transmission channels among the parties should exist to reduce the risk of tapping into the transmission lines.

• Data should be encrypted using algorithms agreed on by the parties involved.

• Electronic signatures should be in the transmissions to identify the source and destination.

• Message authentication codes should exist to ensure that what is sent is received.

The EDI process needs the ability to detect and deal with transactions that do not conform to the standard format or are from/to unauthorized parties.

Options for handling detected errors include requesting retransmissions or manually changing the data.

The critical nature of many EDI transactions, such as orders and payments, requires that there be positive assurances that the transmissions were complete. The transactions need to be successfully passed from the originating computer application to the destination organization. Methods for providing these assurances include internal batch total checking, run-to-run and transmission record count balancing, and use of special acknowledgment transactions for

functional acknowledgments.

Organizations desiring to exchange transactions using EDI are establishing a new business relationship. This business relationship needs to be defined so both parties can conduct business in a consistent and trusting manner. This relationship usually is defined in a legal document called a trading partner agreement. The document should define the transactions to be used, responsibilities of both parties in handling and processing the transactions, and the written business terms and conditions associated with the transactions.

Receipt of Inbound Transactions

Controls should ensure that all inbound EDI transactions are accurately and completely received (communication phase), translated (translation phase), passed to an application (application interface phase), and processed only once.

The control considerations for receipt of inbound transactions are as follows:

• Use appropriate encryption techniques when using public Internet infrastructures for communication in assuring confidentiality, authenticity and integrity of transactions.

• Perform edit checks to identify erroneous, unusual or invalid transactions prior to updating an application.

• Perform additional computerized checking to assess transaction reasonableness, validity, etc. (Consider expert system front ends for complex comparisons.)

• Log each inbound transaction on receipt.

• Use control totals on receipt of transactions to verify the number and value of transactions to be passed to each application; reconcile totals between applications and with trading partners.

• Segment count totals are built into the transaction set trailer by the sender.

• Use control techniques in the processing of individual transactions such as check digits (appended to data to ensure that the original data have not been altered and used to detect transposition and transcription errors) on control

fields, loop or repeat counts.

• Ensure the exchange of control totals of transactions sent and received between trading partners at predefined intervals.

• Maintain a record of the number of messages received/sent and validate

these with the trading partners periodically.

• Arrange for security over temporary files and data transfer to ensure that inbound transactions are not altered or erased between time of transaction receipt and application updates.

Outbound Transactions

Controls should ensure that only properly authorized outbound transactions are processed. This includes the objectives that outbound EDI messages are initiated on authorization, that they contain only preapproved transaction types and that they are sent only to valid trading partners.

The control considerations for outbound transactions are as follows:

• Control the setup and change of trading partner details.

• Compare transactions with trading partner transaction profiles.

• Match the trading partner number to the trading master file (prior to transmission).

• Limit the authority of users within the organization to initiate specific EDI transactions.

• Segregate initiation and transmission responsibilities for high-risk transactions.

• Document management sign-off on programmed procedures and

subsequent changes.

• Log all payment transactions to a separate file, which is reviewed for authorization before transmission.

• Segregate duties within the transaction cycle, particularly where transactions are automatically generated by the system.

• Segregate access to different authorization processes in a transaction cycle.

• Report large (value) or unusual transactions for review prior to or after transmission.

• Log outbound transactions in a secure temporary file until authorized and due for transmission.

• Require paperless authorization that would establish special access to authorization fields (probably two levels, requiring the intervention of different users) within the computer system.

IS Auditor's Role in the EDI Business Process

An IS auditor must evaluate EDI to ensure that all inbound EDI transactions are received and translated accurately, passed to an application, and processed only once.

To accomplish this goal, an IS auditor must review:

• Internet encryption processes put in place to ensure authenticity, integrity, confidentiality and nonrepudiation of transactions

• Edit checks to identify erroneous, unusual or invalid transactions prior to updating the application

• Additional computerized checking to assess transaction reasonableness and validity

• Each inbound transaction to ensure that it is logged on receipt

• The use of control totals on receipt of transactions to verify the number and value of transactions to be passed to each application and reconcile totals between applications and with trading partners

• Segment count totals built into transaction set trailers by the sender

• Transaction set count totals built into the functional group headers by the sender

• Batch control totals built into the functional group headers by the sender

• The validity of the sender against trading partner details by:

– The use of control fields within an EDI message at either the transaction, function, group or interchange level (often within the EDI header, trailer or control record)

– The use of VAN sequential control numbers or reports (if applicable)

– The sending of an acknowledgment transaction to inform the sender of message receipt. The sender should then match this against a file/log of EDI messages sent.

EDI audits also involve:

• **Audit monitors**—Devices can be installed at EDI workstations to capture transactions as they are received. Such transactions can be stored in a protected file for use by the auditor. Consideration should be given to storage requirements for voluminous amounts of data.

• **Expert systems**—Within the context of using the computer system for internal control checks, consideration should be given to having audit monitors evaluate the transactions received. Based upon judgmental rules,

the system can determine the audit significance of such transactions and provide a report for the auditor's use.

Email

Email may be the most heavily used feature of the Internet or local area networks in an organization. At the most basic level, the email process can be divided into two principal components:

• **Mail servers**—Hosts that deliver, forward and store mail

• **Clients**—Interface with users, allowing users to read, compose, send and store

email messages

When a user sends an email message, it is first broken up by the Transmission Control Protocol (TCP) into Internet Protocol (IP) packets.

Those packets are then sent to an internal router, which examines the address and decides whether the mail is to be delivered inside or outside the network.

If the mail is meant for an internal client, the mail is delivered to them. If the mail is to be delivered outside the network, it may pass through a firewall, which will determine if it can be sent or received.

Once out on the Internet, the message is sent to an Internet router, which examines the address and determines where the message should be sent. A gateway at the receiving network receives the email message, which uses TCP to reconstruct the IP packets into a full message and translates the message into the protocol the target network uses. The message may be required to also pass through a firewall on the receiving network. The receiving network examines the email address and sends the message to a specific mailbox.

Binary files can be attached to an email message using encoding. The receiver will have to decode the file once it is received. Email software packages automatically do the encoding for the user and the decoding on the receiving end.

In a closed network, an email has to travel through a series of networks before it reaches the recipient. These networks might use different email formats. Gateways perform the job of translating email formats from one

network to another, so the messages can make their way through all the networks.

The following protocols are the primary protocols an IS auditor will need to be familiar with during the review of email services:

• Outgoing email

– Simple Mail Transport Protocol (SMTP)

• Incoming email

– Post Office Protocol (POP)

– Internet Message Access Protocol (IMAP)

– Hypertext Transfer Protocol (HTTP)—Also called “web-based email”

– Messaging Application Programming Interface (MAPI)—Used with

Outlook in conjunction with a Microsoft Exchange Server mail server; very close to IMAP but has extended features to interact with other applications

Many organizations are moving their email systems to the cloud. This essentially outsources many of the maintenance and security management issues associated with maintaining email servers and shifts expenditures from capital investments to operational expenditures. It also provides additional scalability and availability, which would be more difficult to achieve in smaller IT operations. However, IS auditors must be mindful of the regulatory requirements of their organizations.

Point-of-sale Systems

Point-of-sale (POS) systems enable the capture of data at the time and place that sales transactions occur. The most common payment instruments to operate with POS are credit and debit cards. POS terminals may have attached peripheral equipment—such as optical scanners to read bar codes, magnetic card readers for credit or debit cards, or electronic readers for smart cards—to improve the efficiency and accuracy of the transaction recording process.

It is most important for an IS auditor to determine whether any cardholder data, such as primary account numbers (PANs) or personal identification numbers (PINs), are stored on the local POS system. Any such information, if

stored on the POS system, should be encrypted using strong encryption methods. Certain data, such as card verification value (CVV) numbers, can never be stored on these devices.

Electronic Banking

Financial institutions have been remotely delivering electronic services to consumers and businesses for many years. Risk associated with electronic

banking (ebanking) activities includes strategic, reputational, operational (including security—sometimes called transactional—and legal risk), credit, price, foreign exchange, interest rate and liquidity. Ebanking activities do not raise risk that was not already identified in traditional banking, but ebanking does increase and modify some of types of traditional risk. The core business and the IT environment are tightly coupled, thereby influencing the overall risk profile of ebanking.

An IS auditor is most concerned with strategic, operational and reputational risk because these risk areas are directly related to threats to reliable data flow and operational risk and are certainly heightened by the rapid introduction and underlying technological complexity of ebanking.

Risk Management Challenges

Ebanking presents a number of risk management challenges:

• The speed of change relating to technological and service innovation in ebanking increases the challenge to ensure that adequate strategic assessment, risk analysis and security reviews are conducted prior to implementing new ebanking applications.

• Transactional ebanking websites and associated retail and wholesale business applications are typically integrated as much as possible with legacy computer systems to allow more straight-through processing of electronic transactions. Such straight-through automated processing reduces opportunities for human error and fraud inherent in manual processes, but it also increases dependence on sound system design and architecture as well as system interoperability and operational scalability.

• Ebanking increases a bank’s dependence on information technology, thereby increasing the technical complexity of many operational and security issues and furthering a trend toward more partnerships, alliances

and outsourcing arrangements with third parties such as Internet service providers, telecommunication companies and other technology firms.

• The Internet significantly magnifies the importance of security controls, customer authentication techniques, data protection, audit trail procedures and customer privacy standards.

Risk Management Controls for Ebanking

Effective risk management controls for ebanking include the following controls:

• **Board and management oversight:**

1. Effective management oversight of ebanking activities

2. Establishment of a comprehensive security control process

3. Comprehensive due diligence and management oversight process for outsourcing relationships and other third-party dependencies

• **Security controls:**

1. Authentication of ebanking customers

2. Nonrepudiation and accountability for ebanking transactions

3. Appropriate measures to ensure SoD

4. Proper authorization controls within ebanking systems, databases and applications

5. Data integrity of ebanking transactions, records and information 6. Establishment of clear audit trails for ebanking transactions 7. Confidentiality of key bank information

• **Legal and reputational risk management:**

1. Appropriate disclosures for ebanking services

2. Privacy of customer information

3. Capacity, business continuity and contingency planning to ensure availability of ebanking systems and services

4. Incident response planning

5. Compliance to banking sector directives (e.g., Basel Accords) **Electronic Funds Transfer**

EFT is the electronic transfer of funds between a buyer, a seller and their respective financial institutions. EFT allows parties to move money from one account to another account, replacing traditional check writing and cash collection procedures. EFT transactions usually function via an internal bank

transfer from one party's account to another or via a clearinghouse network.

Transactions originate from a computer at one institution (location) and are transmitted to a computer at another institution (location) with the monetary amount recorded in the respective organization's accounts. Because of the potential high volume of money being exchanged, these systems may be in an extremely high-risk category. Therefore, access security and authorization of processing are important controls. Regarding EFT transactions, central bank requirements should be reviewed for application in these processes.

IS Auditor's Role in the EFT Business Process

Individual consumer access to an EFT system may be controlled by a plastic card and a PIN or by other means that bypass the need for a card. An IS

auditor should review the physical security of unissued plastic cards, the procedures used to generate PINs, the procedures used to issue cards and PINs, and the conditions under which the consumer uses the access devices.

Security in an EFT environment ensures that:

• All the equipment and communication linkages are tested to effectively and reliably transmit and receive data.

• Each party uses security procedures that are reasonably sufficient for affecting the authorized transmission of data and for protecting business records and data from improper access.

• There are guidelines set for the receipt of data and to ensure that the receipt date and time for data transmitted are the date and time the data have been received.

• On receipt of data, the receiving party will immediately transmit an acknowledgment or notification to communicate to the sender that a successful transmission occurred.

• Data encryption standards are set.

• Standards for unintelligible transmissions are set.

• Regulatory requirements for enforceability of electronic data transmitted and received are explicitly stated.

An IS auditor should ensure that reasonable authentication methods are required for access to EFT systems. The communications network should be

designed to provide maximum security. Data encryption is recommended for all transactions; however, an IS auditor should determine any conditions under which the PIN might be accessible in a clear mode.

An EFT switch involved in the network is also an IS audit concern. An EFT

switch is the facility that provides the communication linkage for all equipment in the network. An IS auditor should review the contract with the switch and the third-party audit of the switch operations. If a third-party audit has not been performed, the IS auditor should consider visiting the switch location.

At the application processing level, an IS auditor should review the interface between the EFT system and the application systems that process the accounts from which funds are transferred. Availability of funds or adequacy of credit limits should be verified before funds are transferred. Unfortunately, this is not always the case. Because of the penalties for failure to make a timely transfer, an IS auditor should review backup arrangements or other methods used to ensure continuity of operations. Because EFT reduces the flow of paper and consequently reduces normal audit trails, an IS auditor should determine that alternative audit trails are available.

Automated Teller Machine

An ATM is a specialized form of the POS terminal that is designed for the unattended use by a customer of a financial institution. These machines customarily allow a range of banking and debit operations—especially financial deposits and cash withdrawals. Many ATMs are located in uncontrolled areas to facilitate easy access to customers after hours. They are becoming retail EFT networks, transferring information and money over communication lines. Therefore, the system must provide high levels of logical and physical security

for both the customer and the machinery. The ATM architecture has a physical network layer, a switch and a

communication layer connecting the various ATM POS terminals.

Recommended internal control guidelines for ATMs, apart from what has been provided for any EFT, include the following:

• Written policies and procedures covering personnel, security controls,

operations, disaster recovery credit and check authorization, floor limits, override, settlement, and balancing

• Reconciliation of all general ledger accounts related to retail EFTs and review of exception items and suspense accounts

• Procedures for PIN issuance and protection during storage

• Procedures for the security of PINs during delivery and the restriction of access to a customer's account after a small number of unsuccessful attempts

• Systems designed, tested and controlled to preclude retrieval of stored PINs in any nonencrypted form. Application programs and other software containing formulas, algorithms and data used to calculate PINs must be subject to the highest level of access for security purposes.

• Controls over plastic card procurement, which should be adequate and include a written agreement between the card manufacturer and the bank that details control procedures and methods of resolution to be followed if problems occur

• Controls and audit trails of the transactions that have been made in the ATM. This should include internal registration in the ATM, either in internal paper or digital media, depending on regulation or laws in each country and on the hosts that are involved in the transaction.

IS Auditor's Role in the Use of ATMs

To perform an audit of ATMs, an IS auditor should undertake the following actions:

• Review physical security to prevent introduction of malware.

• Review measures to establish proper customer identification and maintenance of their confidentiality.

• Review file maintenance and retention system to trace transactions.

• Review exception reports to provide an audit trail.

• Review daily reconciliation of ATM transactions including:

– Review SoD in the opening of the ATM and recount of deposit.

– Review the procedures made for the retained cards.

• Review encryption key change management procedures.

– Review physical security measures to ensure security of the ATM and the money contained in the ATM.

– Review the ATM card slot, keypad and enclosure to prevent skimming

of card data and capture of PIN during entry.

Electronic Finance

Electronic finance (efinance) is an integral element of the financial services industry and enables providers to emerge within and across countries, including online banks, brokerages and companies that allow consumers to compare financial services such as mortgage loans and insurance policies.

Nonfinancial entities have also entered the market, including

telecommunication and utility companies that offer payment and other services.

Advantages of this approach to consumers are:

• Lower costs

• Increased breadth and quality

• Widening access to financial services

• Asynchrony (time-decoupled)

• Atopy (location-decoupled)

By using credit scoring and other data mining techniques, providers can create and tailor products over the Internet without much human input and at a very low cost. Providers can better stratify their customer base through analysis of Internet-collected data and allow consumers to build preference profiles online. This not only permits personalization of information and services, it also allows more personalized pricing of financial services and more effective identification of credit risk. At the same time, the Internet allows new financial service providers to compete more effectively for customers because it does not distinguish between traditional brick-and-mortar providers of financial services and those without physical presence.

All these forces are delivering large benefits to consumers at the retail and commercial levels. These mechanisms should be used within privacy law statements (regarding confidentiality and authorization) to gather diverse user information and set up profiles.

Integrated Manufacturing Systems

Integrated manufacturing systems (IMS) have a long history and,

accordingly, there are many models and approaches. Some of the integrated

manufacturing systems include bill of materials (BOM), BOM processing (BOMP), manufacturing resources planning (MRP), computer-assisted design (CAD), computer-integrated (or computer-intensive) manufacturing (CIM), and manufacturing accounting and production (MAP). Original IMSs were based on BOM and BOMP and usually supported by a hierarchical database management system (DBMS).

Evolution toward further integration with other business functions (e.g., recording of raw materials, work-in-process and finished goods transactions, inventory adjustments, purchases, supplier management, sales, accounts payable, accounts receivable, goods received, inspection, invoices, cost accounting, maintenance) led to MRP (initially standing for material requirements

processing, now for manufacturing resources planning), which is a family of widely used standards and standard-based packages. MRP is a typical module of most ERP packages such as SAP or Oracle Financials and is usually integrated in modern customer relationship management (CRM) and supply chain management (SCM) systems.

CAD, computer-assisted engineering (CAE) and computer-assisted

manufacturing (CAM)—the latter including computerized numeric control (CNC)—have led to CIM. CIM is frequently used to run huge lights-out plants, with a significant portion of consumer goods being manufactured in these environments.

The significance to an IS auditor is the high number of systems and applications using these technologies. The larger the scale of integration, the more IS auditor attention is required. Highly integrated CIM projects require the same attention from an IS auditor as the ERPs previously mentioned in this chapter. They are major undertakings that should be based on comprehensive feasibility studies and subject to top management approval and close supervision.

Interactive Voice Response

In telephony, interactive voice response (IVR) is a phone technology that allows a computer to detect voice and touch tones using a normal phone call.

The caller uses the telephone keypad to select from preset menu choices

provided by the IVR. The IVR system then responds with prerecorded or dynamically generated audio to further direct callers or route the caller to a customer service representative. IVR systems can be used to control almost any function in which the interface can be broken down into a series of simple menu choices. IVR systems generally scale well to handle large call volumes.

An IS auditor should ensure that there are controls over such systems in place to prevent unauthorized individuals from entering system-level commands that may permit them to change or rerecord menu options.

Purchase Accounting System

Financial transactions are frequently processed through more than one system.

For example, in a retail store, a sale is first processed in the sales accounting system, then processed by the accounts receivable system (if the purchase was by credit card) and, for either cash or credit sales, through the inventory system (when they are linked). That same sale might trigger the purchase accounting system to replace depleted inventory. Eventually the transactions become part of the general ledger system because all transactions are recorded somewhere in that system. For the integration of systems to be effective, processing of a financial transaction must be complete, accurate and timely. If it is not, a ripple effect impairs the integrity of the data.

Purchase accounting systems process the data for purchases and payments.

Because purchases automatically lead to payments, if purchases are properly contracted, partial control over payments exists. Additional controls over payments are also required to ensure that each payment was made for goods and services received, that the same purchase was not paid for twice, and that they were, indeed, paid. Most purchase accounting systems perform three basic accounting functions:

1. **Accounts payable processing**—Recording transactions in the accounts payable records

2. **Goods received processing**—Recording details of goods received but not yet invoiced

3. **Order processing**—Recording goods ordered but not yet received

Image Processing

Some of the many algorithms used in image processing include convolution (on which many others are based), fast Fourier transform (FFT), discrete cosine transform (DCT), thinning (or skeletonization), edge detection and contrast enhancement. These are usually implemented in software but may also use special-purpose hardware for speed.

An imaging system stores, retrieves and processes graphic data, such as pictures, charts and graphs, instead of or in addition to text data. The storage capacities must be enormous, and most image systems include optical disk storage. In addition to optical disks, the systems include high-speed scanning, high-resolution displays, rapid and powerful compression, communications functions,

and laser printing. The systems include techniques that can identify levels of shades and colors that cannot be differentiated by the human eye.

These systems are expensive, and companies do not invest in them lightly.

Most businesses that perform image processing obtain benefits from using the imaging system. Examples of potential benefits are:

• Item processing (e.g., signature storage and retrieval)

• Immediate retrieval via a secure optical storage medium

• Increased productivity

• Improved control over paper files

• Reduced deterioration due to handling

• Enhanced disaster recovery procedures

The replacement of paper documents with electronic images can have a significant impact on the way an organization does business. Many of the traditional controls for paper-based systems may be reduced or absent in electronic documentation workflow. New controls must be developed and designed into the automated process to ensure that information image files cannot be altered, erased or lost.

Risk areas that management should address when installing imaging systems and that an IS auditor should be aware of when reviewing an institution's controls over imaging systems include:

• **Planning**—The lack of careful planning in selecting and converting paper

systems to document imaging systems can result in excessive installation costs, the destruction of original documents and the failure to achieve expected benefits. Critical issues include converting existing paper storage files and integration of the imaging system into the organization workflow and electronic media storage to meet audit and document retention legal requirements.

• **Audit**—Imaging systems may change or eliminate the traditional controls as

well as the checks and balances inherent in paper-based systems. Audit procedures may have to be redesigned and new controls designed into the automated process.

• **Redesign of workflow**—Institutions generally redesign or reengineer workflow processes to benefit from imaging technology.

• **Scanning devices**—Scanning devices are the entry point for image documents and a significant risk area in imaging systems. They can disrupt workflow if the scanning equipment is not adequate to handle the volume of documents or the equipment breaks down. The absence of controls over the scanning process can result in poor quality images, improper indexing, and incomplete or forged documents being entered into the system.

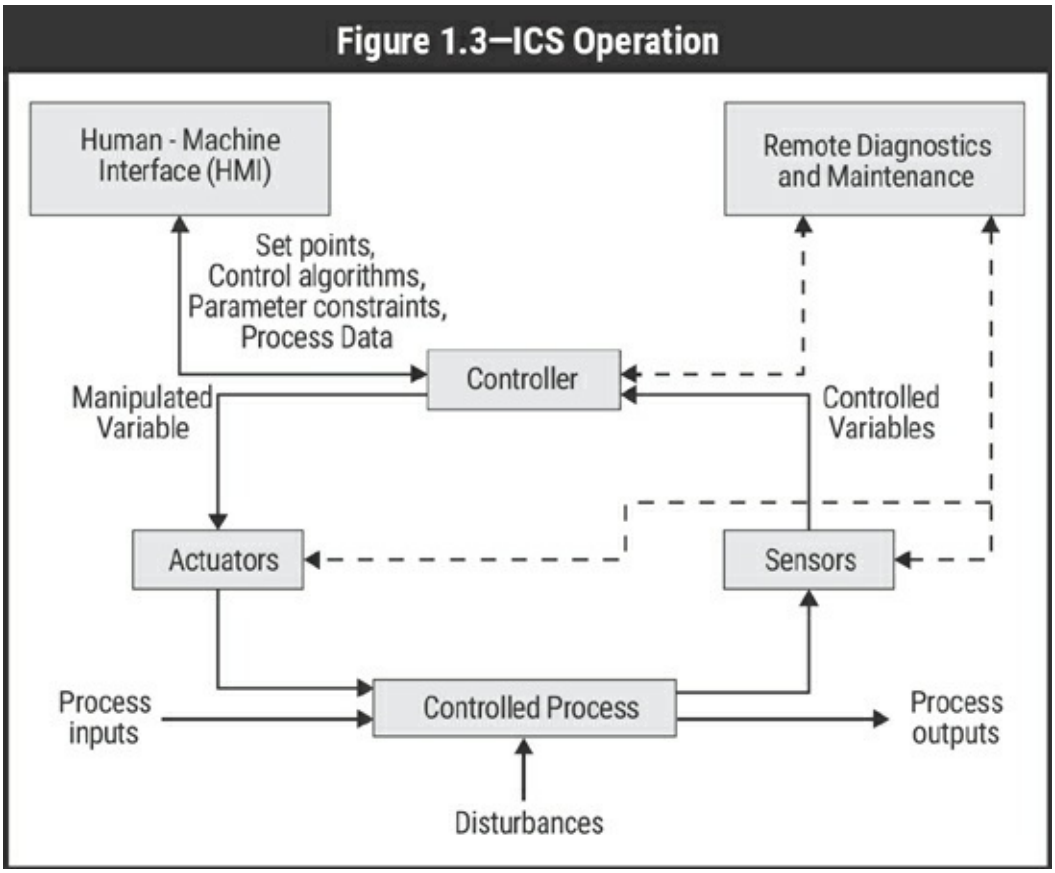
Procedures should be in place to ensure that original documents are not destroyed before determining that a good image has been captured.

• **Software security**—Security controls over image system documents are critical to protect institutions and customer information from unauthorized access and modifications. The integrity and reliability of the imaging system database are related directly to the quality of controls over access to the system.

• **Training**—Inadequate training of personnel scanning the documents can result in poor-quality document images and indexes, and the early destruction of original documents. The installation and use of imaging systems can be a major change for department personnel. They must be trained adequately to ensure quality control over the scanning and storage of imaging documents as well as the use of the system to maximize the benefits of converting to imaging systems.

Industrial Control Systems

Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition



(SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC), often found in the industrial sectors and critical infrastructures.

Figure 1.3 provides a high-level overview of typical ICS process flows.

Source: NIST; *NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security*, USA, 2011

Risk Factors

Based on the criticality that ICSs have on manufacturing, chemical processes and, more important, critical infrastructure (energy generation, transmission and control, water treatment, etc.), there are key risk factors that an IS auditor must consider:

• Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation

• Unauthorized changes to instructions, commands or alarm thresholds, which could damage, disable or shut down equipment, create

environmental impacts, and/or endanger human life

• Inaccurate information sent to system operators, either to disguise unauthorized changes or to cause the operators to initiate inappropriate actions, which could have various negative effects

• ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects

• Interference with the operation of safety systems, which could endanger human life

Typical Controls

To address risk, the following controls should be considered within the administrative, operational and technical implementation of ICS:

• Restricting logical access to the ICS network and network activity. This includes using a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and ICS networks and having separate authentication

mechanisms and credentials for users of the corporate and ICS networks.

The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.

• Restricting physical access to the ICS network and devices. Unauthorized physical access to components could cause serious disruption of the ICS's functionality. A combination of physical access controls should be used, such as locks, card readers and/or guards.

• Protecting individual ICS components from exploitation. This includes deploying security patches in as expeditious a manner as possible, after testing them under field conditions; disabling all unused ports and services; restricting ICS user privileges to only those that are required for each person's role; tracking and monitoring audit trails; and using security controls such as antivirus

software and file integrity checking software, where technically feasible, to prevent, deter, detect and mitigate malware.

• Maintaining functionality during adverse conditions. This involves designing the ICS so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event.

• Restoring the system after an incident. Incidents are inevitable, and an incident response plan is essential. A major characteristic of a good security program is how quickly a system can be recovered after an incident has occurred.

Artificial Intelligence and Expert Systems

Artificial intelligence (AI) is the study and application of the principles by which:

• Knowledge is acquired and used.

• Goals are generated and achieved.

• Information is communicated.

• Collaboration is achieved.

• Concepts are formed.

• Languages are developed.

AI fields include, among others:

• Expert systems

• Natural and artificial (such as programming) languages

• Neural networks

• Intelligent text management

• Theorem proving

• Abstract reasoning

• Pattern recognition

• Voice recognition

• Problem solving

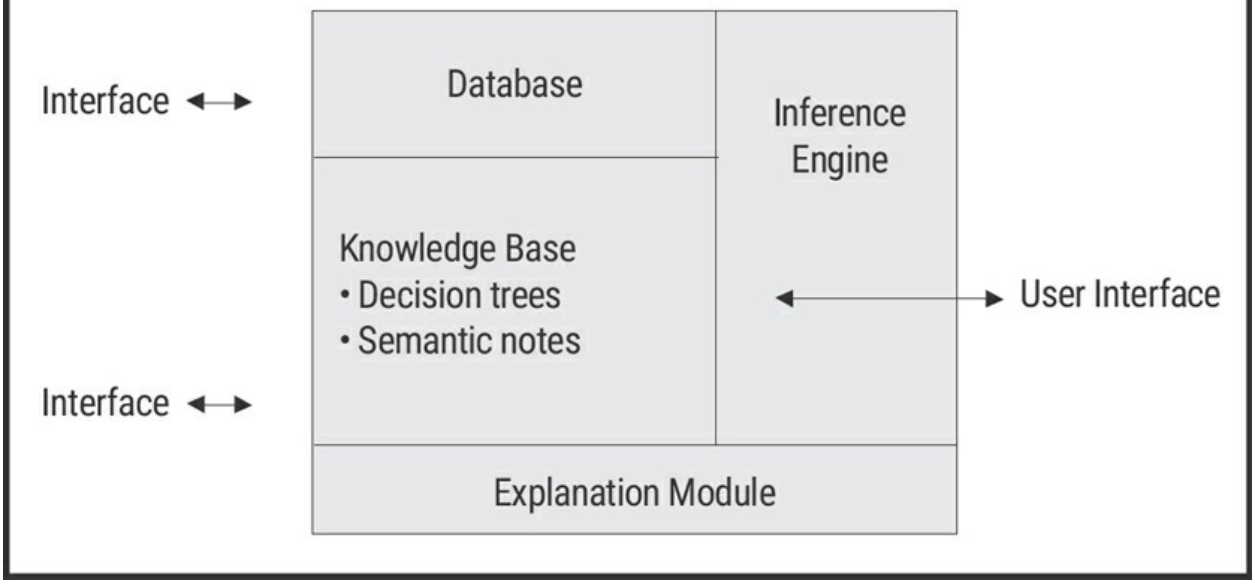
• Machine translation of foreign languages

Expert systems are an area of AI and perform a specific function or are prevalent in certain industries. An expert system allows the user to specify certain basic assumptions or formulas and then uses these assumptions or formulas to analyze arbitrary events. Based on the information used as input to the system, a conclusion is produced.

The use of expert systems has many potential benefits within an organization including:

• Capturing the knowledge and experience of individuals

Figure 1.4—Artificial Intelligence Expert Systems



• Sharing knowledge and experience

• Enhancing personnel productivity and performance

• Automating highly (statistically) repetitive tasks (help desk, score credits, etc.)

• Operating in environments where a human expert is not available (e.g., medical assistance on board of a ship, satellites)

Expert systems are comprised of the primary components shown in **figure**

1.4, called shells when they are not populated with particular data, and the

shells are designed to host new expert systems.

Key to the system is the knowledge base (KB), which contains specific information or fact patterns associated with particular subject matter and the rules for interpreting these facts. The KB interfaces with a database in obtaining data to analyze a particular problem in deriving an expert conclusion. The information in the KB can be expressed in several ways:

• **Decision trees**—Use of questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

• **Rules**—Expression of declarative knowledge through the use of if-then relationships. For example, if a patient's body temperature is over 39°C

(102.2°F) and their pulse is under 60, then the patient might be suffering from a certain disease.

• **Semantic nets**—Use of a graph in which the nodes represent physical or conceptual objects and the arcs describe the relationship between the nodes. Semantic nets resemble a data flow diagram and make use of an inheritance mechanism to prevent duplication of data. Additionally, the inference engine shown is a program that uses the KB and determines the most appropriate outcome based on the information supplied by the user. In addition, an expert system includes the following components:

– **Knowledge interface**—Inclusion of knowledge from an expert into the system without the traditional mediation of a software engineer

– **Data interface**—Collection of data from nonhuman sources through an expert system, such as measurement instruments in a power plant

An explanation module that is user-oriented in addressing the problem is analyzed, and the expert conclusion reached is also provided.

IS Auditor's Role in Expert Systems

Well-designed questionnaires or software that integrates and reports on system parameters and data sets are available to assist IS auditors in reviewing these systems. Other accounting-and auditing-related applications for expert systems include audit planning, internal control analysis, account attribute analysis, quality review, accounting decisions, tax planning and user training. Consistent with standard systems development methodologies, stringent change control procedures should be followed because the basic assumptions and formulas may need to be changed as more expertise is gained. As with other systems, access should be on a need-to-know basis.

An IS auditor should be knowledgeable about the various AI and expert system applications used within the organization. An IS auditor needs to be concerned with the controls relevant to these systems when used as an integral part of an organization's business process or mission-critical functions, and the level of experience or intelligence used as a basis for developing the software. This is critical because errors produced by AI systems may have a more severe impact than those produced by traditional systems. This is true especially of intelligent systems that facilitate healthcare

professionals in the diagnosis and treatment of injuries and illnesses. Error loops/routines should be designed into these systems.

Specifically, an IS auditor should perform the following activities:

• Understand the purpose and functionality of the system.

• Assess the system's significance to the organization and related businesses processes as well as the associated potential risk.

• Review the adherence of the system to corporate policies and procedures.

• Review the decision logic built into the system to ensure that the expert knowledge or intelligence in the system is sound and accurate. An IS

auditor should ensure that the proper level of expertise was used in developing

the basic assumptions and formulas.

• Review procedures for updating information in the KB.

• Review security access over the system, specifically the KB.

• Review procedures to ensure that qualified resources are available for maintenance and upgrading.

Supply Chain Management

Supply chain management (SCM) is linking the business processes between the related entities such as the buyer and the seller. The link is provided to all the connected areas such as managing logistics and the exchange of information, services and goods among supplier, consumer, warehouse, wholesale/retail distributors and the manufacturer of goods.

SCM has become a focal point and is seen as a new area in strategic management because of the shift in the business scenario at the advent of global competition, proliferation of the Internet, the instantaneous transmission of information and web presence in all spheres of business activities. SCM includes managing the flow of goods, services and information among suppliers, manufacturers, wholesalers, distributors, stores, consumers and end users.

SCM shifts the focus; all the entities in the supply chain can work collaboratively and in real time, thus reducing, to a great extent, the required available inventory. The just-in-time (JIT) concept becomes possible, and the cycle time is reduced with an objective of reducing unneeded inventory.

Seasonal (e.g., both availability and demand) and regional (e.g., preferences in size, shape, quantity) factors are addressed.

Stock levels of nonmoving items are significantly reduced, and there is an automated flow of supply and demand. Also, the intrinsic costs and errors associated with the manual means such as fax, input of data, delay and inaccurate orders, can be avoided.

Customer Relationship Management

The customer-driven business trend is to be focused on the wants and needs of

the customers. This emphasizes the importance of focusing on information relating to transaction data, preferences, purchase patterns, status, contact history, demographic information and service trends of customers, rather than on products.

All these factors lead CRM, which is an optimum combination of strategy, tactics, processes, skill sets and technology. CRM has become a strategic success factor for all types of business, and its proficiency has a significant impact on profitability.

Customer-centered applications focus on CRM processes emphasizing the customer, rather than marketing, sales or any other function in order to meet customer expectations. This includes integration of telephony, web and database technologies, and interenterprise integration capabilities. In this model, other business partners can share information, communicate and collaborate with the organization with the seamless integration of web-enabled applications and without changing their local network and other configurations.

It is possible to distinguish between operational and analytical CRM.

Operational CRM is concerned with maximizing the utility of the customer's service experience while also capturing useful data about the customer interaction. Analytical CRM seeks to analyze information captured by the organization about its customers and their interactions with the organization into information that allows greater value to be obtained from the customer base. Among uses of analytical CRM are increasing customer product

holdings or "share of customer wallet," moving customers into higher margin products, moving customers to lower-cost service channels, increasing marketing success rates, and making pricing decisions.

1.2.6 USING THE SERVICES OF OTHER AUDITORS AND EXPERTS

Due to the scarcity of IS auditors and the need for IT security specialists and other subject matter experts to conduct audits of highly specialized areas, the audit department or auditors entrusted with providing assurance may require the services of other auditors or experts. Outsourcing of IS assurance and security services is increasingly becoming a common practice.

External experts could include experts in specific technologies such as networking, automated teller machines, wireless, systems integration and digital forensics, or subject matter experts such as specialists in a particular industry or area of specialization such as banking, securities trading, insurance or the law.

When a part or all of IS audit services are proposed to be outsourced to another audit or external service provider, the following should be considered with regard to using the services of other auditors and experts:

• Restrictions on outsourcing of audit/security services provided by laws and regulations

• Audit charter or contractual stipulations

• Impact on overall and specific IS audit objectives

• Impact on IS audit risk and professional liability

• Independence and objectivity of other auditors and experts

• Professional competence, qualifications and experience

• Scope of work proposed to be outsourced and approach

• Supervisory and audit management controls

• Method and modalities of communication of results of audit work

• Compliance with legal and regulatory stipulations

• Compliance with applicable professional standards

Based on the nature of assignment, the following may also require special consideration:

• Testimonials/references and background checks

• Access to systems, premises and records

• Confidentiality restrictions to protect customer-related information

• Use of computer-assisted auditing techniques (CAATs) and other tools to be used by the external audit service provider

• Standards and methodologies for performance of work and documentation

• Nondisclosure agreements

The IS auditor or entity outsourcing the auditing services should monitor the relationship to ensure the objectivity and independence throughout the duration of the arrangement. It is important to understand that although a part of or the whole of the audit work may be delegated to an external service provider, the related professional liability is not necessarily delegated.

Therefore, it is the responsibility of the IS auditor or entity employing the services of external service providers to do the following:

• Clearly communicate the audit objectives, scope and methodology through a formal engagement letter.

• Establish a monitoring process for regular review of the work of the external service provider with regard to planning, supervision, review and documentation. For example, the work papers of other IS auditors or experts should be reviewed to confirm the work was appropriately planned, supervised, documented and reviewed and to consider the appropriateness and sufficiency of the audit evidence provided. Likewise, the reports of other IS auditors or experts should be reviewed to confirm the scope specified in the audit charter, terms of reference or letter of engagement has been met, that any significant assumptions used by other IS auditors or experts have been identified, and the findings and conclusions reported have been agreed on by management.

• Assess the usefulness and appropriateness of reports of such external providers and assess the impact of significant findings on the overall audit objectives.

Note: The IS auditor should be familiar with ISACA Audit and Assurance Standard 1203 Performance and Supervision and the IS Audit and

Assurance Guideline 2206 Using the Work of Other Experts, focusing on

the rights of access to the work of other experts.

1.3 TYPES OF CONTROLS

Every organization has controls in place. An effective control is one that prevents, detects and/or contains an incident and enables recovery from a risk event. Organizations design, develop, implement and monitor information systems through policies, procedures, practices and organizational structures to address these types of risk.

Controls are normally composed of policies, procedures, practices and organizational structures that are implemented to reduce risk to the organization. Internal controls are developed to provide reasonable assurance to management that the organization's business objectives will be achieved, and risk events will be prevented, or detected and corrected. Internal control activities and supporting processes are either manual or automated. Internal controls operate at all levels within an organization to mitigate its exposures to risk that potentially could prevent it from achieving its business objectives.

The board of directors and senior management are responsible for establishing the appropriate culture to facilitate an effective and efficient internal control system and for continuously monitoring the effectiveness of the internal control system, although each individual within an organization must take part in this process.

There are two key aspects that controls should address:

• What should be achieved

• What should be avoided

Internal controls address business/operational objectives and should also address undesired events through prevention, detection and correction.

Elements of controls that should be considered when evaluating control strength are classified as preventive, detective or corrective in nature.

Figure 1.5 describes control classifications, functions and usages.

Note: A CISA candidate should understand the purpose of and differences between preventive, detective and corrective controls and be able to recognize examples of each.

1.3.1 CONTROL OBJECTIVES AND CONTROL MEASURES

A control objective is defined as an objective of one or more operational area(s) or role(s) to be achieved in order to contribute to the fulfillment of strategic goal(s) of the company. That is, the control objective is such a goal that is explicitly related to the strategy of the company.

Control objectives are statements of the desired result or purpose to be achieved by implementing control activities (procedures). For example, control objectives may relate to the following concepts:

• Effectiveness and efficiency of operations

Figure 1.5—Control Classifications

Class	Function	Examples
Preventive	• Detect problems before they arise • Employing only qualified personnel • Monitor both operation and inputs • Segregation of duties • Attempt to predict potential problems • Controlling access to physical facilities	before they occur and make • Well-designed documents to prevent

adjustments

errors

• Prevent an error, omission or malicious

• Suitable procedures for authorization of

act from occurring

transactions

• Programmed edit checks

• Use of access control software that

allows only authorized personnel to

access sensitive files

• Use of encryption software to prevent

unauthorized disclosure of data

Detective

• Use controls that detect and report the

• Hash totals

occurrence of an error, omission or

• Check points in production jobs

malicious act

• Echo controls in telecommunications

• Error messages over tape labels

• Duplicate checking of calculations

• Periodic performance reporting with variances

• Past-due account reports

• Internal audit functions

• Review of activity logs to detect unauthorized access attempts

• Secure code reviews

• Software quality assurance

Corrective

• Minimize the impact of a threat

• Contingency/continuity of operations

• Remedy problems discovered by planning

detective controls

• Disaster recovery planning

• Identify the cause of a problem

• Incident response planning

• Correct errors arising from a problem

• Backup procedures

• Modify the processing system(s) to

• System break/fix service level

minimize future occurrences of the

agreements

problem

• Reliability of financial reporting

• Compliance with applicable laws and regulations

• Safeguarding assets

Control objectives apply to all controls, whether they are manual, automated or a combination (e.g., review of system logs). Control objectives in an IS

environment do not differ from those in a manual environment; however, the way these controls are implemented may be different. Thus, control objectives need to be addressed relevant to specific IS-related processes.

A control measure is defined as an activity contributing to the fulfillment of a control objective. Both the control objective and control measure serve the decomposition of the strategic-level goals into such lower-level goals and activities that can be assigned as tasks to the staff. This assignment can take the form of a role description in a job description.

IS Control Objectives

IS control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process area. IS

control objectives are:

• Statements of the desired result or purpose to be achieved by implementing controls around information systems processes

• Comprised of policies, procedures, practices and organizational structures

• Designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, or detected and corrected

Organizational management needs to make choices relative to these control

objectives by doing the following:

• Selecting those that are applicable

• Deciding on those that will be implemented

• Choosing how to implement them (frequency, span, automation, etc.)

• Accepting the risk of not implementing those that may apply

Specific IS control objectives include the following:

• Safeguarding assets: information on automated systems being up to date and secure from improper access

• Ensuring system development life cycle (SDLC) processes are established, in place and operating effectively to provide reasonable assurance that business, financial and/or industrial software systems and applications are developed in a repeatable and reliable manner to assure business objectives are met

• Ensuring integrity of general OS environments, including network management and operations

• Ensuring integrity of sensitive and critical application system environments, including accounting/financial and management information (information objectives) and customer data, through:

– Authorization of the input. Each transaction is authorized and entered only once.

– Validation of the input. Each input is validated and will not cause negative impact to the processing of transactions.

– Accuracy and completeness of processing of transactions. All

transactions are recorded accurately and entered into the system for the proper period.

– Reliability of overall information processing activities

– Accuracy, completeness and security of the output

– Database confidentiality, integrity and availability

• Ensuring appropriate identification and authentication of users of IS

resources (end users as well as infrastructure support)

• Ensuring the efficiency and effectiveness of operations (operational objectives)

• Complying with users' requirements, organizational policies and procedures, and applicable laws and regulations (compliance objectives)

• Ensuring availability of IT services by developing efficient business continuity plans (BCPs) and disaster recovery plans (DRPs) that include backup and recovery processes

• Enhancing protection of data and systems by developing an incident response plan

• Ensuring integrity and reliability of systems by implementing effective change management procedures

• Ensuring that outsourced IS processes and services have clearly defined service level agreements (SLAs) and contract terms and conditions to ensure the organization's assets are properly protected and meet business goals and objectives

1.3.2 EVALUATION OF THE CONTROL ENVIRONMENT

An IS auditor reviews evidence gathered during the audit to determine if the operations reviewed are well controlled and effective. This is also an area that requires judgment and experience. An IS auditor also assesses the strengths and weaknesses of the controls evaluated and determines if they are effective in meeting the control objectives established as part of the audit planning process.

A control matrix is often used in assessing the proper level of controls.

Known types of errors that can occur in an area under review are placed on the top axis of the matrix and known controls to detect or correct errors are placed on the side axis of the matrix. Then, using a ranking method, the matrix is filled with the appropriate measurements. When completed, the matrix illustrates areas

where controls are weak or lacking.

In some instances, a strong control may compensate for a weak control in another area. For example, if an IS auditor finds weaknesses in a system's transaction error report, a detailed manual balancing process over all transactions may be in place to compensate for the weaknesses in the error report. An IS auditor should be aware of compensating controls in areas where controls have been identified as weak.

While a compensating control situation occurs when one stronger control supports a weaker one, overlapping controls are two strong controls. For

example, if a data center employs a card key system to control physical access and a guard inside the door requires employees to show their card key or badge, an overlapping control exists. Either control might be adequate to restrict access, but the two complement each other.

Normally, a control objective will not be achieved by considering one control adequate. Rather, an IS auditor will perform a variety of testing procedures and evaluate how these relate to one another.

Generally, a group of controls, when aggregated together, may act as compensating controls, and thereby minimize the risk. An IS auditor should always review for compensating controls prior to reporting a control weakness.

An IS auditor may not find each control procedure to be in place but should evaluate the comprehensiveness of controls by considering the strengths and weaknesses of control procedures.

1.3.3 GENERAL CONTROLS

General controls apply to all areas of an organization and include the following:

• Internal accounting controls that are primarily directed at accounting operations —controls that concern the safeguarding of assets and reliability of financial records

• Operational controls that concern day-to-day operations, functions and activities, and ensure that the operation is meeting the business objectives

• Administrative controls that concern operational efficiency in a functional area and adherence to management policies (administrative controls support the operational controls specifically concerned with these areas)

• Organizational security policies and procedures to ensure proper usage of assets

• Overall policies for the design and use of adequate documents and records (manual/automated) to help ensure proper recording of transactions—

transactional audit trail

• Procedures and practices to ensure adequate safeguards over access to and use of assets and facilities

• Physical and logical security policies for all facilities, data centers and IT

resources (e.g., servers and telecom infrastructure)

1.3.4 IS-SPECIFIC CONTROLS

Each general control can be translated into an IS-specific control. A well-designed information system should have controls built in for all its sensitive or critical functions. For example, the general procedure to ensure that adequate safeguards over access to assets and facilities can be translated into an IS-related set of control procedures, covering access safeguards over computer programs, data and equipment.

IS control procedures include:

• Strategy and direction of the IT function

• General organization and management of the IT function

• Access to IT resources, including data and programs

• Systems development methodologies and change control

• Operations procedures

• Systems programming and technical support functions

• Quality assurance (QA) procedures

• Physical access controls

• BCP/DRP

• Networks and communication technology (e.g., local area networks, wide area networks, wireless)

• Database administration

• Protection and detective mechanisms against internal and external attacks
Note: A CISA candidate should understand concepts regarding IS controls and how to apply them in planning an audit.

1.4 RISK-BASED AUDIT PLANNING

Risk-based audit planning is the deployment of audit resources to areas within an organization that represent the greatest risk. It requires an understanding of the organization and its environment, specifically:

• External and internal factors affecting the organization

• The organization's selection and application of policies and procedures

• The organization's objectives and strategies

• Measurement and review of the organization's performance

As part of obtaining this understanding, an IS auditor must also gain an understanding of the key components of the organization's:

• Strategy management

• Business products and services

• Corporate governance process

• Transaction types, transaction partners and transaction flows within information systems

Effective risk-based auditing uses risk assessment to drive the audit plan and minimize the audit risk during the execution of an audit.

A risk-based audit approach is used to assess risk and to assist an IS auditor in making the decision to perform either compliance testing or substantive testing. It is important to stress that the risk-based audit approach efficiently assists an IS auditor in determining the nature and extent of testing.

Within this concept, inherent risk, control risk or detection risk should not be of major concern, despite some weaknesses. In a risk-based audit approach, IS auditors are not just relying on risk; they also rely on internal and operational controls as well as knowledge of the organization or the business.

This type of risk assessment decision can help relate the cost-benefit analysis of the control to the known risk, allowing practical choices.

Business risk includes concerns about the probable effects of an uncertain event on achieving established business objectives. The nature of business risk may be financial, regulatory or operational and may also include risk derived from specific technology. For example, an airline company is subject to extensive safety regulations and economic changes, both of which impact the continuing operations of the company. In this context, the availability of IT service and its reliability are critical. Risk also includes those measures an organization is willing to take in order to achieve or advance their objectives, but the results may be unproven or uncertain.

By understanding the nature of the business, an IS auditor can identify and categorize the types of risk that will better determine the risk model or approach in conducting the audit. The risk model assessment can be as simple as creating weights for the types of risk associated with the business and identifying the risk in an equation. On the other hand, risk assessment can be a scheme where risk has been given elaborate weights based on the nature of the business or the significance of the risk. A simplistic overview of a risk-based audit approach can be seen in **figure 1.6**.

1.4.1 AUDIT RISK AND MATERIALITY

Audit risk can be defined as the risk that information collected may contain a material error that may go undetected during the course of the audit. An IS

auditor should also consider, if applicable, other factors relevant to the organization: customer data, privacy, availability of provided services, and corporate and public image, as in the case of public organizations or foundations.

Audit risk is influenced by:

• **Inherent risk**—As it relates to audit risk, it is the risk level or exposure of the process/entity to be audited without considering the controls that management has implemented. Inherent risk exists independent of an audit and can occur because of the nature of the business.

• **Control risk**—The risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls.

For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often easily missed due to the volume of logged information. The control risk associated with computerized data validation procedures is ordinarily low if the processes are consistently applied.

• **Detection risk**—The risk that material errors or misstatements that have occurred will not be detected by an IS auditor.

• **Overall audit risk**—The probability that information or financial reports may contain material errors and that the auditor may not detect an error that has occurred. An objective in formulating the audit approach is to limit the audit risk in the area under scrutiny so the overall audit risk is at a

sufficiently low level at the completion of the examination.

An internal control weakness or set of combined internal control weaknesses may leave an organization highly susceptible to the occurrence of a threat (e.g., financial loss, business interruption, loss of customer trust, economic sanction). An IS auditor should be concerned with assessing the materiality of the items in question through a risk-based audit approach to evaluating internal controls.

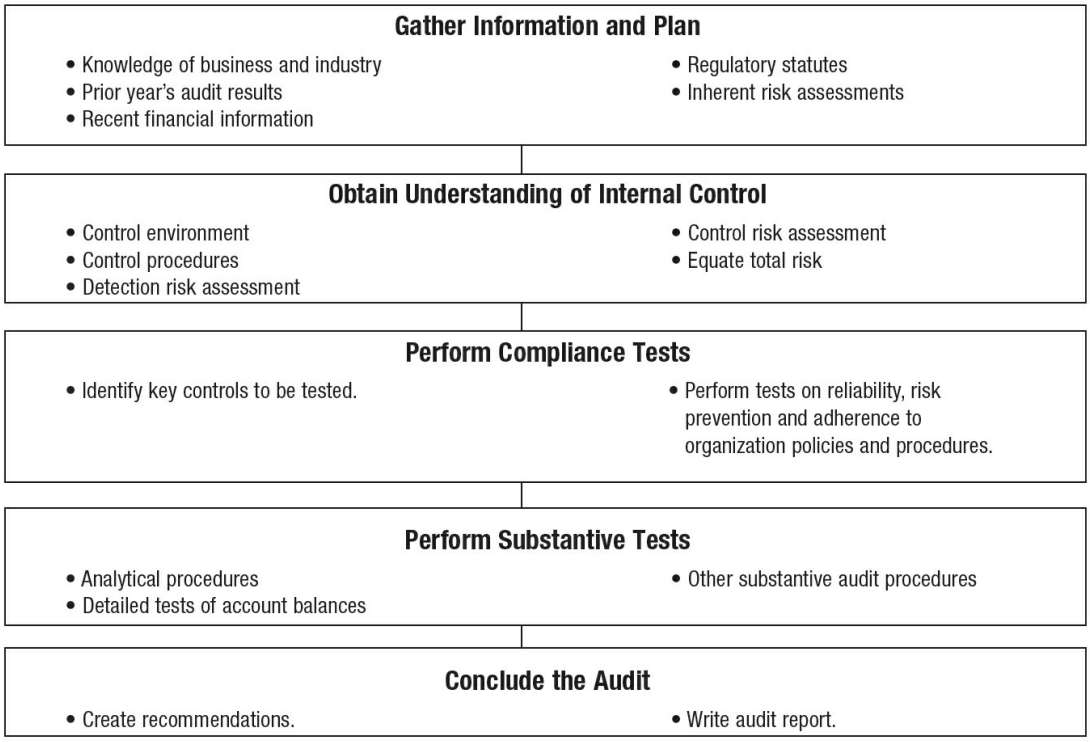
An IS auditor should have a good understanding of audit risk when planning an audit. An audit sample may not detect every potential error in a population. However, by using proper statistical sampling procedures or a strong quality control process, the probability of detection risk can be reduced to an acceptable

level.

Similarly, when evaluating internal controls, an IS auditor should realize that a given system may not detect a minor error. However, that specific error, combined with others, could become material to the overall system.

Note: A CISA candidate should understand audit risk and not confuse it with statistical sampling risk, which is the risk that incorrect assumptions are made about the characteristics of a population from which a sample is selected.

Figure 1.6—Risk-based Audit Approach



Note: For further guidance, see standard 1204 Materiality and guideline 2204 Materiality.

1.4.2 RISK ASSESSMENT

An IS auditor should understand how the organization being audited approaches risk assessment. Risk assessments should identify, quantify and prioritize risk against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action, priorities for managing information security risk and priorities for implementing controls selected to protect against risk.

Risk assessments should be performed periodically to address changes in the environment, security requirements, and the risk situation (e.g., in the assets, threats, vulnerabilities, impacts), and when significant changes occur. These should be performed methodically and be capable of producing comparable and reproducible results.

The scope of a risk assessment can be the entire organization; parts of the organization; an individual information system; specific system components; or

services where this is practicable, realistic and helpful.

In order to address risk, an organization should establish the criteria for determining whether risk can be managed within the risk appetite. Risk may be accepted if, for example, it is assessed that the risk is low or the cost of treatment is not cost-effective for the organization. Such decisions should be recorded.

Risk identified in the risk assessment needs to be treated. Possible risk response options include:

• **Risk mitigation**—Applying appropriate controls to reduce the risk

• **Risk acceptance**—Knowingly and objectively not taking action, provided the risk clearly satisfies the organization's policy and criteria for risk acceptance

• **Risk avoidance**—Avoiding risk by not allowing actions that would cause the risk to occur

• **Risk sharing (transfer)**—Transferring the associated risk to other parties (e.g., insurers or suppliers)

For risk for which the risk treatment option is to apply appropriate controls, controls should be selected to ensure that risk is reduced to an acceptable level, considering the following:

• Requirements and constraints of national and international legislation and regulations

• Organizational objectives

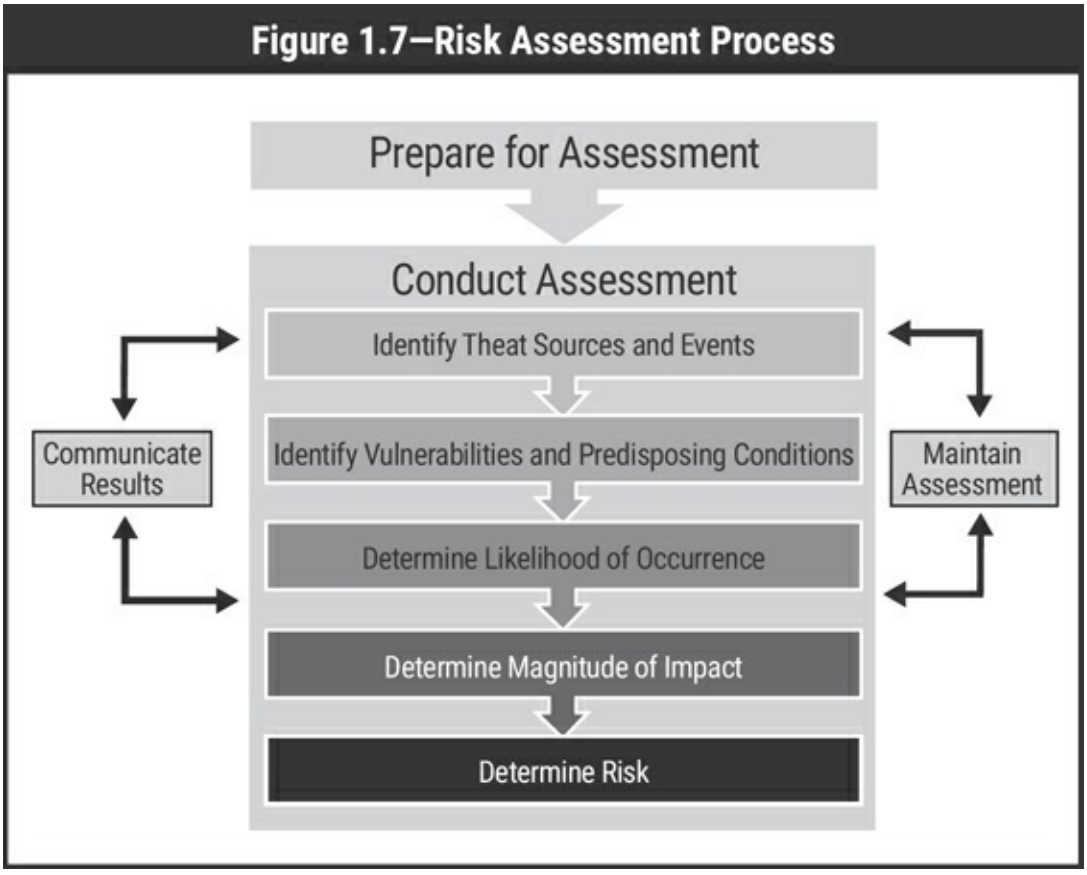
• Operational requirements and constraints

• Cost-effectiveness (the need to balance the investment in implementation and operation of controls against the harm likely to result from security failures)

From an IS auditor's perspective, risk assessment serves several purposes:

• Assisting an IS auditor in identifying risk and threats to an IT environment and IS system—risk and threats that would need to be addressed by management—and in identifying system-specific internal controls.

Depending on the level of risk, this assists an IS auditor in selecting certain



areas to examine.

• Helping an IS auditor in the evaluation of controls in audit planning

• Assisting an IS auditor in determining audit objectives

• Supporting risk-based audit decision making

Figure 1.7 depicts the specific processes used by an IS auditor to realize these objectives.

Source: National Institute of Standards and Technology (NIST), *NIST Special Publication 800-30, Revision 1: Information Security*, USA, 2012. Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

When developing the overall IS audit plan, a suitable risk assessment approach

should be followed. To correctly and completely assess the risk that is related to the complete scope of the IS audit area, an IS auditor should consider the following elements when developing the IS audit plan:

• Full coverage of all areas within the scope of the IS audit universe, which represents the range of all possible audit activities

• Reliability and suitability of the risk assessment provided by management

• The processes followed by management to supervise, examine and report possible risk or issues

• Coverage of risk in related activities relevant to the activities under review

1.4.3 IS AUDIT RISK ASSESSMENT TECHNIQUES

When determining which functional areas should be audited, an IS auditor may face a large variety of audit subjects. Each of these subjects may represent different types of risk. An IS auditor should evaluate these various risk candidates to determine the high-risk areas that should be audited.

There are many risk assessment methodologies from which an IS auditor may choose. These range from simple classifications based on the IS auditor’s judgment of high, medium and low, to complex scientific calculations that provide a numeric risk rating.

One such risk assessment approach is a scoring system that is useful in prioritizing audits based on an evaluation of risk factors. The system considers variables such as technical complexity, level of control procedures in place and level of financial loss. These variables may or may not be weighted. The risk values are then compared to each other, and audits are scheduled accordingly.

Another form of risk assessment is subjective, in which an independent decision is made based on business knowledge, executive management directives, historical perspectives, business goals and environmental factors.

A combination of techniques can be used. Risk assessment methods may change and develop over time to best serve the needs of the organization. An IS auditor should consider the level of complexity and detail appropriate for the organization being audited.

Using risk assessment to determine areas to be audited results in the following outcomes:

• Enabling audit management to effectively allocate limited audit resources

• Ensuring that relevant information has been obtained from all levels of management, including boards of directors, IS auditors and functional area

management. Generally, this information assists management in effectively discharging its responsibilities and ensures that the audit activities are directed to high-risk areas, which will add value for management.

• Establishing a basis for effectively managing the audit department

• Providing a summary of how the individual audit subject is related to the overall organization as well as to the business plans

1.4.4 RISK ANALYSIS

Risk analysis is a subset of risk assessment and is used during audit planning to help identify risk and vulnerabilities so an IS auditor can determine the controls needed to mitigate risk. Risk assessment procedures provide a basis for the identification and assessment of risk of material vulnerabilities; however, they do not provide sufficient appropriate audit evidence on which to base the audit opinion.

In evaluating IT-related business processes applied by an organization, it is important to understand the relationship between risk and control. IS auditors must be able to identify and differentiate risk types and the controls used to mitigate this risk. They should have knowledge of common business risk areas, related technology risk and relevant controls. They should also be able to evaluate the risk assessment and management process and techniques used by business managers, and to make assessments of risk to help focus and plan audit work. In addition to an understanding of business risk and control, IS

auditors must understand that risk exists within the audit process.

Risk is defined as the combination of the probability of an event and its consequence *(International Organization for Standardization [ISO]*

31000:2009: Risk management—Principles and guidelines/ISO Guide 73:2009: Risk management—Vocabulary). Business risk may negatively impact the assets, processes or objectives of a specific business or organization. An IS auditor is often focused on high-risk issues associated with the confidentiality, integrity or availability of sensitive and critical information and the underlying information systems and processes that generate, store and manipulate such information. In reviewing these types of IT-related business risk, an IS auditor will often assess the effectiveness of the risk management process an organization uses.

In analyzing the business risk arising from the use of IT, it is important for an IS auditor to have a clear understanding of the following aspects:

• Industry and/or internationally accepted risk management processes

• The purpose and nature of business, the environment in which the business operates and related business risk

• Dependence on technology in the achievement of business goals and objectives

• The business risk of using IT and how it impacts the achievement of the business goals and objectives

• A good overview of the business processes and the impact of IT and related risk on the business process objectives

The risk assessment process is an iterative life cycle that begins with identifying business objectives; information assets; and the underlying systems or information resources that generate, store, use or manipulate the assets (e.g., hardware, software, databases, networks, facilities, people) critical to achieving these objectives. Because IT risk is dynamic, management should recognize the need for and establish an adaptive IT risk management process that supports the business risk management process. As a result, the most effort can be directed toward the most sensitive or critical assets to the organization. Next, a risk assessment is performed to identify vulnerabilities and threats and determine the probability of occurrence and the resulting impact and additional safeguards that would mitigate this impact to a level acceptable to management.

During the risk mitigation phase, controls are identified for treating the identified risk. These controls should prevent or reduce the likelihood of a risk event occurring, detect the occurrence of a risk event, minimize the impact or transfer

the risk to another organization.

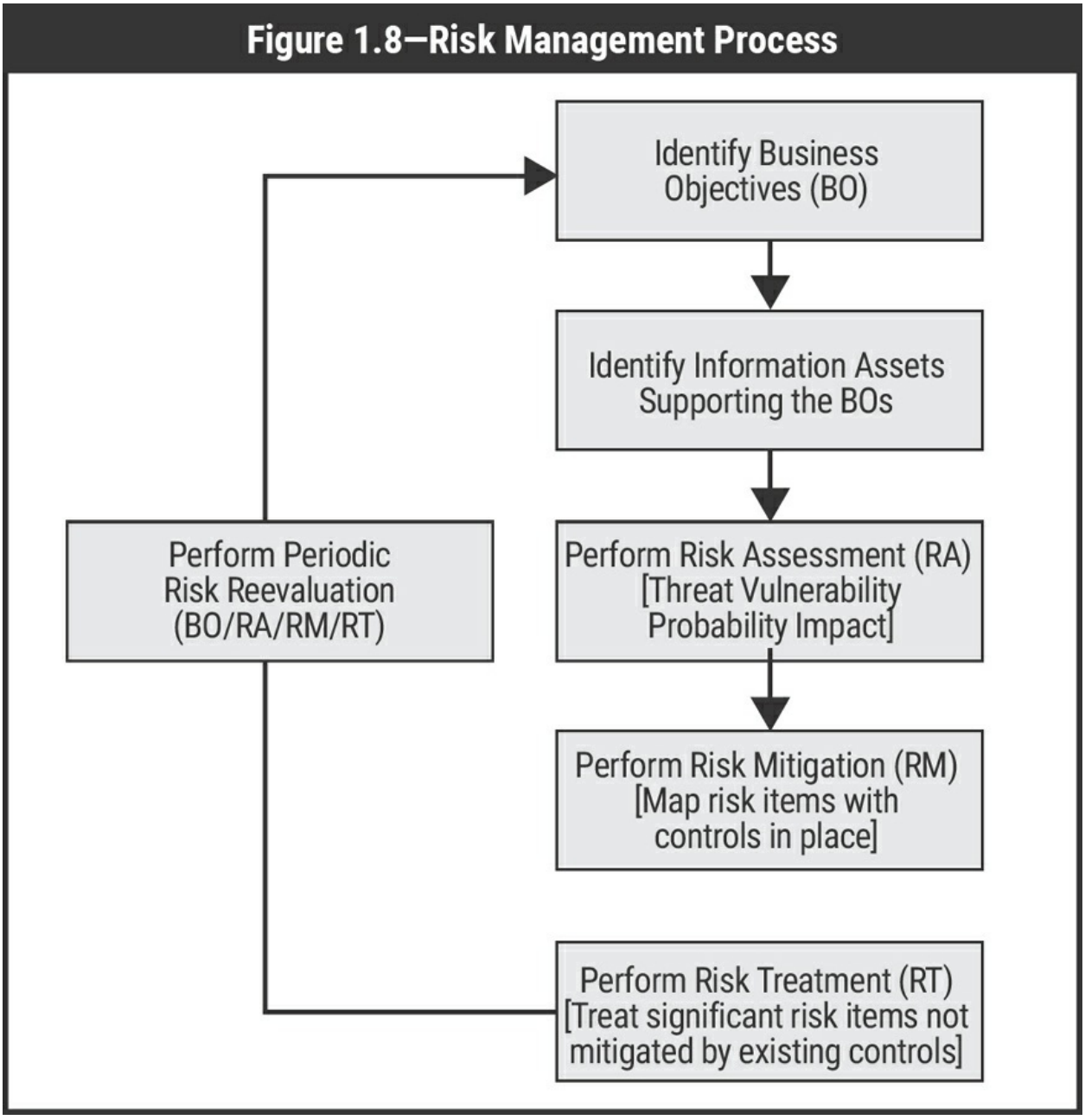
The assessment of countermeasures should be performed through a cost-benefit analysis where controls are selected to reduce risk to a level acceptable to management. This process may be based on the following:

• The cost of the control compared to the benefit of minimizing the risk

• Management’s risk appetite (i.e., the level of residual risk that management is prepared to accept)

• Preferred risk-reduction methods (e.g., terminate the risk, minimize probability of occurrence, minimize impact, transfer the risk via insurance) The final phase relates to monitoring performance levels of the risk being managed, identifying any significant changes in the environment that would trigger a risk reassessment, warranting changes to its control environment. It encompasses three processes—risk assessment, risk mitigation and risk reevaluation—in determining whether risk is being mitigated to a level acceptable to management. It should be noted that, to be effective, risk assessment should be an ongoing process in an organization that endeavors to continually identify and evaluate risk as it arises and evolves. See **figure 1.8**

for the summary of the risk management process.



1.5 TYPES OF AUDITS AND ASSESSMENTS

An IS auditor should understand the various types of audits that can be performed, internally or externally, and the basic audit procedures associated with each. These include:

• **IS audit**—An IS audit is designed to collect and evaluate evidence to determine whether an information system and related resources are adequately safeguarded and protected; maintain data and system integrity

and availability; provide relevant and reliable information; achieve organizational goals effectively; consume resources efficiently; and have, in effect, internal controls that provide reasonable assurance that business, operational and control objectives will be met and undesired events will be prevented, or detected and corrected, in a timely manner.

• **Compliance audit**—A compliance audit includes specific tests of controls to demonstrate adherence to specific regulatory or industry-specific standards or practices. These audits often overlap other types of audits but may focus on particular systems or data.

• **Financial audit**—A financial audit assesses the accuracy of financial reporting. A financial audit will often involve detailed, substantive testing, although IS auditors are increasingly placing more emphasis on a risk- and control-based audit approach. This kind of audit relates to financial information integrity and reliability.

• **Operational audit**—An operational audit is designed to evaluate the internal control structure in a given process or area. An IS audit of application controls or logical security systems are examples of an operational audit.

• **Integrated audit**—There are a number of different types of integrated audits, but typically an integrated audit combines financial and operational audit steps and may or may not include the use of an IS auditor. An integrated audit is also performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and compliance. An integrated audit can be performed by external or internal auditors and would include compliance tests of internal controls and substantive audit steps. See section 1.11, Quality Assurance and Improvement of the Audit Process, for more info.

• **Administrative audit**—An administrative audit is designed to assess issues related to the efficiency of operational productivity within an organization.

• **Specialized audit**—Many different types of specialized audits are conducted. Within the category of IS audit, specialized reviews may examine areas such as fraud or services performed by third parties.

– **Third-party service audit**—A third-party service audit addresses the audit of outsourced financial and business processes to third-party service providers,

which may operate in different jurisdictions. A third-

party service audit issues an opinion on a service organization's description of controls through a service auditor's report, which then can be used by the IS auditor of the entity that uses the services of the service organization.

– **Fraud audit**—A fraud audit is a specialized audit designed to discover fraudulent activity. Auditors often use specific tools and data analysis techniques to discover fraud schemes and business irregularities.

– **Forensic audit**—A forensic audit is a specialized audit to discover, disclose and follow up on fraud and crime. The primary purpose of such an audit is the development of evidence for review by law enforcement and judicial authorities.

• **Computer forensic audit**—A computer forensic audit is an investigation that includes the analysis of electronic devices such as computers, smartphones, disks, switches, routers and hubs. An IS auditor possessing the necessary skills can assist an information security manager or forensic specialist in performing forensic investigations and conduct an audit of the system to ensure compliance with the evidence collection procedures for forensic investigation.

• **Functional audit**—A functional audit provides an independent evaluation of software products, verifying that its configuration items' actual functionality and performance are consistent with the requirement specifications. Specifically, this audit is held prior to the software delivery or after implementation.

PART B: EXECUTION

Once an audit is planned and the scope and objectives are defined, the IS

auditor is ready to execute the audit plan. The following sections provide guidance for executing an audit.

1.6 AUDIT PROJECT MANAGEMENT

Several steps are required to perform an audit. Adequate planning is a necessary first step in performing effective IS audits. To efficiently use IS

audit resources, audit organizations must assess the overall risk for the general and application areas and related services being audited, and then develop an

audit program that consists of objectives and audit procedures to satisfy the audit objectives. The audit process requires an IS auditor to gather evidence, evaluate the strengths and weaknesses of controls based on the evidence gathered through audit tests, and prepare an audit report that presents to management those issues (i.e., areas of control weaknesses with recommendations for remediation) in an objective manner.

Audit management must ensure the availability of adequate audit resources and a schedule for performing the audits and, in the case of internal IS audit, for follow-up reviews on the status of corrective actions taken by management. The process of auditing includes defining the audit scope, formulating audit objectives, identifying audit criteria, performing audit procedures, reviewing and evaluating evidence, forming audit conclusions and opinions, and reporting to management after discussion with key process owners.

Project management techniques for managing and administering audit projects include the following basic steps:

• **Plan the audit engagement**—Plan the audit, considering project-specific risk.

• **Build the audit plan**—Chart out the necessary audit tasks across a

timeline, optimizing resource use. Make realistic estimates of the time requirements for each task with proper consideration given to the availability of the auditee.

• **Execute the plan**—Execute audit tasks against the plan.

• **Monitor project activity**—Report actual progress against planned audit steps to ensure challenges are managed proactively and the scope is completed within time and budget.

1.6.1 AUDIT OBJECTIVES

Audit objectives refer to the specific goals that must be accomplished by the audit. In contrast, a control objective refers to how an internal control should function. An audit generally incorporates several audit objectives.

Audit objectives often focus on confirming that internal controls exist to minimize business risk and they function as expected. These audit objectives

include assuring compliance with legal and regulatory requirements as well as the confidentiality, integrity, reliability and availability of information and IT resources. Audit management may give an IS auditor a general control objective to review and evaluate when performing an audit.

A key element in planning an IS audit is to translate basic and wide-ranging audit objectives into specific IS audit objectives. For example, in a financial/operational audit, a control objective could be to ensure that transactions are properly posted to the general ledger accounts. However, in an IS audit, the objective could be extended to ensure that editing features are in place to detect errors in the coding of transactions that may impact the account-posting activities.

An IS auditor must understand how general audit objectives can be translated into specific IS control objectives. Determining an audit's objectives is a critical step in planning an IS audit.

One of the primary purposes of an IS audit is to identify control objectives and the related controls that address the objective. For example, an IS

auditor's initial review of an information system should identify key controls.

It should then be determined whether to test these controls for compliance.

An IS auditor should identify both key general and application controls after developing an understanding and documenting the business processes and the applications/functions that support these processes and general support systems. Based on that understanding, an IS auditor should identify the key control points.

Alternatively, an IS auditor may assist in assessing the integrity of financial reporting data, referred to as substantive testing, through CAATs.

1.6.2 AUDIT PHASES

Each phase in the execution of an audit can be divided into key steps to plan, define, perform and report the results, as shown in **figure 1.9**.

These steps can be further broken down into more specific activities, as shown in **figure 1.10**.

1.6.3 AUDIT PROGRAMS

An audit program is a step-by-step set of audit procedures and instructions that should be performed to complete an audit. It is based on the scope and objective of the particular assignment.

The main purposes of developing an audit program are to accomplish the following:

• Formal documentation of audit procedures and sequential steps

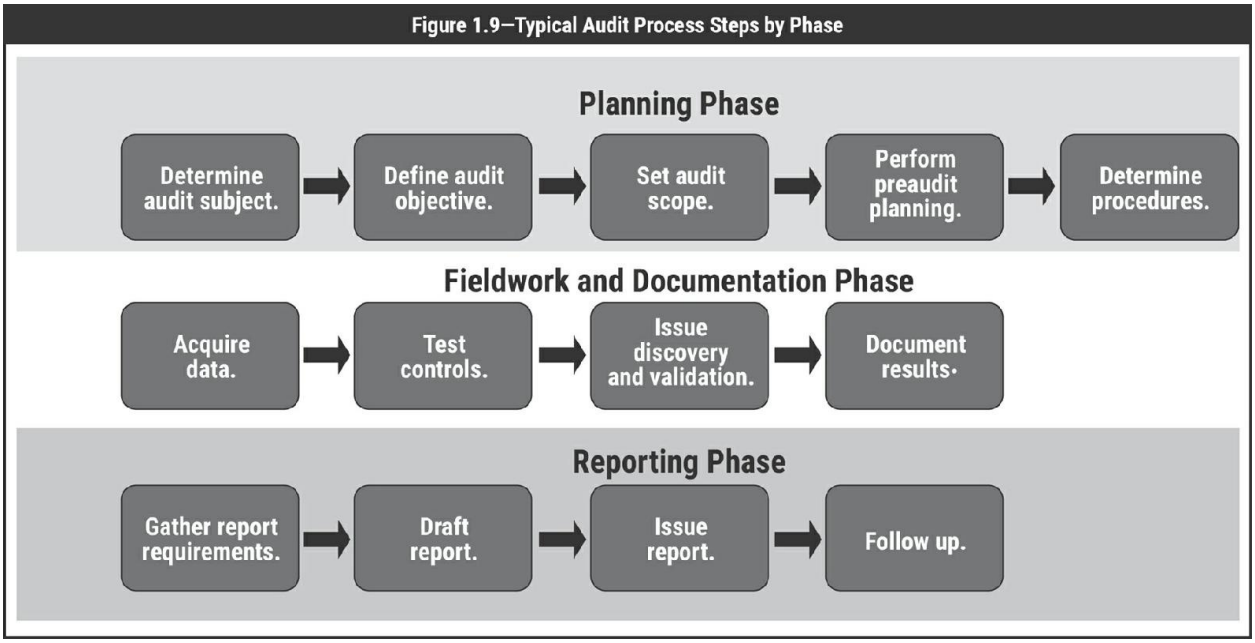
• Creation of procedures that are repeatable and easy to use by internal or external audit and assurance professionals who need to perform similar audits

• Documentation of the type of testing that will be used (compliance and/or substantive)

• Meeting generally accepted audit standards that relate to the planning phase in the audit process

An IS auditor often evaluates IT functions and systems from different perspectives, such as security (confidentiality, integrity and availability), quality (effectiveness, efficiency), fiduciary (compliance, reliability), service and capacity. The audit work program is the audit strategy and plan—it

Figure 1.9—Typical Audit Process Steps by Phase



identifies scope, audit objectives and audit procedures to obtain sufficient, relevant and reliable evidence to draw and support audit conclusions and opinions.

Source: ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, USA, 2016

Figure 1.10—Audit Process Activities by Step

Audit Step

Description

1. Determine audit subject.

Identify the area to be audited (e.g., business function, system, physical location).

2. Define audit objective.

Identify the purpose of the audit. For example, an objective

might be to determine whether program source code changes

occur in a well-defined and controlled environment.

3. Set audit scope.

Identify the specific systems, function or unit of the organization to be included in the review. For example, in the previous

example (program changes), the scope statement might limit the

review to a single application, system or a limited period of

time.

This step is very important because the IS auditor will need to

understand the IT environment and its components to identify

the resources that will be required to conduct a comprehensive

evaluation. A clear scope will help the IS auditor define a set of testing points that is relevant to the audit and further determine the technical skills and resources necessary to evaluate different technologies and their components.

4. Perform preaudit planning.

• Conduct a risk assessment, which is critical in setting the final scope of a risk-based audit. For other types of audits (e.g.,

compliance), conducting a risk assessment is a good practice

because the results can help the IS audit team to justify the

engagement and further refine the scope and preplanning

focus.

• Interview the auditee to inquire about activities or areas of

concern that should be included in the scope of the

engagement.

• Identify regulatory compliance requirements.

• Once the subject, objective and scope are defined, the audit

team can identify the resources that will be needed to perform

the audit work. Some of the resources to be defined follow:

– Technical skills and resources needed

– Budget and effort needed to complete the engagement

– Locations or facilities to be audited

– Roles and responsibilities among the audit team

– Time frame for the various stages of the audit

– Sources of information for test or review, such as functional flowcharts, policies, standards, procedures and prior audit work papers

– Points of contact for administrative and logistics arrangements

– A communication plan that describes to whom to communicate, when, how often and for what purposes

5. Determine audit procedures

At this stage of the audit process, the audit team should have and steps for data gathering.

enough information to identify and select the audit approach or strategy and start developing the audit program. Some of the specific activities in this step are:

• Identify and obtain departmental policies, standards and guidelines for review.

• Identify any regulatory compliance requirements.

• Identify a list of individuals to interview.

• Identify methods (including tools) to perform the evaluation.

• Develop audit tools and methodology to test and verify

controls.

• Develop test scripts.

• Identify criteria for evaluating the test.

• Define a methodology to evaluate that the test and its results are accurate (and repeatable if necessary).

Source: ISACA, *Information Systems Auditing: Tools and Techniques—*

Creating Audit Programs, USA, 2016

General audit procedures are the basic steps in the performance of an audit and usually include:

• Obtaining and recording an understanding of the audit area/subject

• Creating a risk assessment and general audit plan and schedule

• Performing detailed audit planning that includes the necessary audit steps and a breakdown of the work planned across an anticipated time line

• Doing a preliminary review of the audit area/subject

• Evaluating the audit area/subject

• Verifying and evaluating the appropriateness of controls designed to meet control objectives

• Conducting compliance testing (tests of the implementation of controls and their consistent application)

• Conducting substantive testing (confirming the accuracy of information)

• Reporting (communicating results)

• Following up in cases where there is an internal audit function **Minimum Skills to Develop an Audit Program**

Developing meaningful audit and assurance programs depends on the ability to customize audit procedures according to the nature of the subject under review and the specific risk that must be addressed in the audit area/organization. The following skills can assist an IS auditor in creating an audit program:

• Good understanding of the nature of the enterprise and its industry to identify and categorize the types of risk and threat

• Good understanding of the IT space and its components and sufficient knowledge of the technologies that affect them

• Understanding of the relationship between business risk and IT risk

• A basic knowledge of risk assessment practices

• Understanding of the different testing procedures for evaluating IS controls and identifying the best method of evaluation, for example:

– The use of generalized audit software to survey the contents of data files (e.g., system logs, user access list)

– The use of specialized software to assess the contents of operating systems, databases and application parameter files

– Flowcharting techniques for documenting business processes and automated controls

– The use of audit logs and reports to evaluate parameters

– Review of documentation

– Inquiry and observations

– Walk-throughs

– Reperformance of controls

Note: For additional guidance, see standard 1203 Performance and Supervision and guideline 2203 Performance and Supervision.

1.6.4 AUDIT WORK PAPERS

All audit plans, programs, activities, tests, findings and incidents should be properly documented in work papers. The format and media of work papers can vary, depending on specific needs of the department. IS auditors should particularly consider how to maintain the integrity and protection of audit test evidence in order to preserve its value as substantiation in support of audit results.

Work papers can be considered the bridge or interface between the audit objectives and the final report. Work papers should provide a seamless transition —with traceability and support for the work performed—from objectives to report and from report to objectives. In this context, the audit report can be viewed as a particular work paper.

1.6.5 FRAUD, IRREGULARITIES AND ILLEGAL ACTS

Management is primarily responsible for establishing, implementing and maintaining an internal control system that leads to the deterrence and/or timely detection of fraud. Internal controls may fail where such controls are circumvented by exploiting vulnerabilities or through management-perpetrated weakness in controls or collusion among people.

The presence of internal controls does not altogether eliminate fraud. IS

auditors should observe and exercise due professional care in all aspects of their work and be alert to the possible opportunities that allow fraud to materialize. They should be aware of the possibility and means of perpetrating fraud, especially by exploiting the vulnerabilities and overriding controls in the IT-enabled environment. They should have knowledge of

fraud and fraud indicators and be alert to the possibility of fraud and errors while performing an audit.

During the course of regular assurance work, an IS auditor may come across instances or indicators of fraud. After careful evaluation, an IS auditor may communicate the need for a detailed investigation to appropriate authorities.

In the case of the IS auditor identifying a major fraud or if the risk associated with the detection is high, audit management should also consider communicating in a timely manner to the audit committee.

Regarding fraud prevention, an IS auditor should be aware of potential legal requirements concerning the implementation of specific fraud detection procedures and reporting fraud to appropriate authorities.

Note: For additional guidance, see standard 1207 Irregularity and Illegal Acts and guideline 2207 Irregularity and Illegal Acts.

1.7 SAMPLING METHODOLOGY

Valid conclusions can be reached using audit sampling. When using either statistical or nonstatistical sampling methods, IS auditors should design and select an audit sample, perform audit procedures and evaluate sample results to obtain sufficient and appropriate evidence to form a conclusion. When using sampling methods to draw a conclusion on the entire population, professionals should use statistical sampling.

An IS auditor should consider the purpose of the sample:

• **Compliance testing/test of controls**—An audit procedure designed to evaluate the operating effectiveness of controls in preventing, or detecting and correcting, material weaknesses

• **Substantive testing/test of details**—An audit procedure designed to detect material weaknesses at the assertion level

1.7.1 COMPLIANCE VERSUS SUBSTANTIVE TESTING

Compliance testing is evidence gathering for the purpose of testing an

organization’s compliance with control procedures. This differs from substantive testing in which evidence is gathered to evaluate the integrity of individual transactions, data or other information.

A compliance test determines whether controls are being applied in a manner that complies with management policies and procedures. For example, if an IS auditor is concerned about whether production program library controls are

working properly, the IS auditor might select a sample of programs to determine whether the source and object versions are the same. The broad objective of any compliance test is to provide reasonable assurance that the particular control as perceived in the preliminary evaluation.

It is important that an IS auditor understand the specific objective of a compliance test and of the control being tested. Compliance tests can be used to test the existence and effectiveness of a defined process, which may include a trail of documentary and/or automated evidence—for example, to provide assurance that only authorized modifications are made to production programs.

A substantive test substantiates the integrity of actual processing. It provides evidence of the validity and integrity of the balances in the financial statements and the transactions that support these balances. An IS auditor could use substantive tests to test for monetary errors directly affecting financial statement balances or other relevant data of the organization.

Additionally, an IS auditor might develop a substantive test to test the completeness and accuracy of report data. To perform this test, the IS auditor might use a statistical sample, which will allow the IS auditor to develop a conclusion regarding the accuracy of all of the data.

A direct correlation exists between the level of internal controls and the amount of substantive testing required. If the results of testing controls (compliance tests) reveal the presence of adequate internal controls, then minimizing the substantive procedures could be justified. Conversely, if the control testing reveals weaknesses in controls that may raise doubts about the completeness, accuracy or validity of the accounts, substantive testing can alleviate those doubts.

Examples of compliance testing of controls where sampling could be considered include user access rights, program change control procedures, documentation procedures, program documentation, follow-up of exceptions, review of logs and software license audits.

Examples of substantive tests where sampling could be considered include performance of a complex calculation (e.g., interest) on a sample of accounts or a sample of transactions to vouch for supporting documentation.

An IS auditor could also decide during the preliminary assessment of the

controls to include some substantive testing if the results of this preliminary evaluation indicate that implemented controls are not reliable or do not exist.

Figure 1.11 shows the relationship between compliance and substantive tests and describes the two categories of substantive tests.

Note: A CISA candidate should be knowledgeable on when to perform compliance tests or substantive tests.

1.7.2 SAMPLING

Sampling is performed when time and cost considerations preclude a total verification of all transactions or events in a predefined population. The population consists of the entire group of items that need to be examined. The subset of population members used to perform testing is called a sample.

Sampling is used to infer characteristics about a population based on the characteristics of a sample.

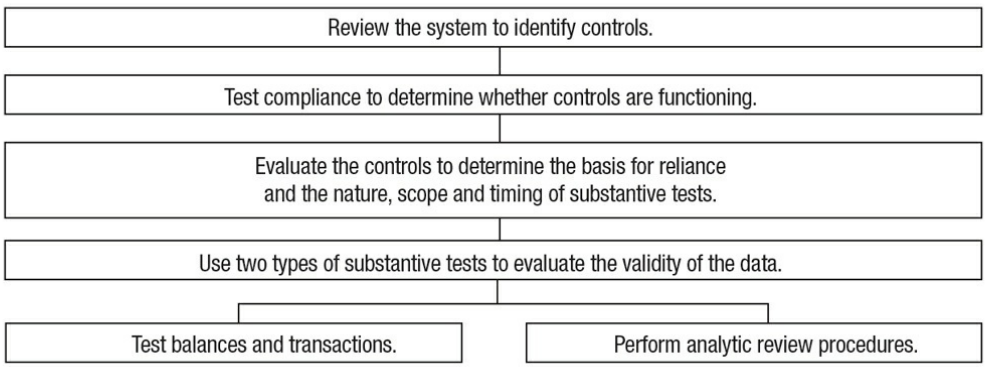
The two general approaches to audit sampling are statistical and nonstatistical:

• **Statistical sampling**—An objective method of determining the sample size and selection criteria

– Statistical sampling uses the mathematical laws of probability to: (1) calculate the sampling size, (2) select the sample items, and (3) evaluate the sample results and make the inference.

– With statistical sampling, an IS auditor quantitatively decides how

Figure 1.11—Understand the Control Environment and Flow of Transactions



closely the sample should represent the population (assessing sample precision) and the number of times in 100 that the sample should represent the population (the reliability or confidence level). This assessment is represented as a percentage. The results of a valid statistical sample are mathematically quantifiable.

• **Nonstatistical sampling (often referred to as judgmental sampling)—**

Uses audit judgment to determine the method of sampling, the number of items that will be examined from a population (sample size) and which items to select (sample selection)

– These decisions are based on subjective judgment as to which

items/transactions are the most material and most risky.

When using either statistical or nonstatistical sampling methods, an IS auditor should design and select an audit sample, perform audit procedures and evaluate sample results to obtain sufficient, reliable, relevant and useful audit evidence. These methods of sampling require an IS auditor to use judgment when defining the population characteristics and, thus, are subject to the risk that incorrect conclusions could be drawn from the sample (sampling risk).

However, statistical sampling permits an IS auditor to quantify the probability of error (confidence coefficient). To be a statistical sample, each item in the population should have an equal opportunity or probability of being selected. Within these two general approaches to audit sampling, there are two primary methods of sampling used—attribute sampling and variable sampling. Attribute sampling, generally applied in compliance testing, deals

with the presence or absence of the attribute and provides conclusions that are expressed in rates of incidence. Variable sampling, generally applied in substantive testing, deals with population characteristics that vary, such as monetary values and weights (or any other measurement), and provides conclusions related to deviations from the norm.

Attribute sampling refers to three different, but related, types of proportional sampling:

• **Attribute sampling (also referred to as fixed sample-size attribute**

sampling or frequency-estimating sampling)—A sampling model that is used to estimate the rate (percent) of occurrence of a specific quality (attribute) in a population. Attribute sampling answers the question of

"how many?" An example of an attribute that might be tested is approval signatures on computer access request forms.

• **Stop-or-go sampling**—A sampling model that helps prevent excessive sampling of an attribute by allowing an audit test to be stopped at the earliest possible moment. Stop-or-go sampling is used when an IS auditor believes that relatively few errors will be found in a population.

• **Discovery sampling**—A sampling model most often used when the objective of the audit is to seek out (discover) fraud, circumvention of regulations or other irregularities. For example, if the sample is found to be error free, it is assumed that no fraud/irregularity exists; however, if a single error is found, the entire sample is believed to be

fraudulent/irregular.

Variable sampling—also known as dollar estimation or mean estimation sampling—is a technique used to estimate the monetary value or some other unit of measure (such as weight) of a population from a sample portion. An example of variable sampling is a review of an organization's balance sheet for material transactions and an application review of the program that produced the balance sheet.

Variable sampling refers to three types of quantitative sampling models:

• **Stratified mean per unit**—A statistical model in which the population is divided into groups and samples are drawn from the various groups; used to produce a smaller overall sample size relative to unstratified mean per

unit

• **Unstratified mean per unit**—A statistical model in which a sample mean is calculated and projected as an estimated total

• **Difference estimation**—A statistical model used to estimate the total difference between audited values and book (unaudited) values based on

differences obtained from sample observations

The following statistical sampling terms need to be understood:

• **Confidence coefficient (also referred to as confidence level or reliability factor)**—A percentage expression (90 percent, 95 percent, 99 percent, etc.) of the probability that the characteristics of the sample are a true representation of the population. Generally, a 95 percent confidence coefficient is considered a high degree of comfort. If an IS auditor knows internal controls are strong, the confidence coefficient may be lowered.

The greater the confidence coefficient, the larger the sample size.

• **Level of risk**—Equal to one minus the confidence coefficient. For example, if the confidence coefficient is 95 percent, the level of risk is five percent (100 percent minus 95 percent).

• **Precision**—Set by an IS auditor, it represents the acceptable range difference between the sample and the actual population. For attribute sampling, this figure is stated as a percentage. For variable sampling, this figure is stated as a monetary amount or a number. The higher the precision amount, the smaller the sample size and the greater the risk of fairly large total error amounts going undetected. The smaller the precision amount, the greater the sample size. A very low precision level may lead to an unnecessarily large sample size.

• **Expected error rate**—An estimate stated as a percent of the errors that may exist. The greater the expected error rate, the greater the sample size.

This figure is applied to attribute sampling formulas but not to variable sampling formulas.

• **Sample mean**—The sum of all sample values, divided by the size of the sample. The sample mean measures the average value of the sample.

• **Sample standard deviation**—Computes the variance of the sample values from the mean of the sample. Sample standard deviation measures the spread or dispersion of the sample values.

• **Tolerable error rate**—Describes the maximum misstatement or number of

errors that can exist without an account being materially misstated.

Tolerable rate is used for the planned upper limit of the precision range for compliance testing. The term is expressed as a percentage. “Precision range” and “precision” have the same meaning when used in substantive testing.

• **Population standard deviation**—A mathematical concept that measures the relationship to the normal distribution. The greater the standard deviation, the larger the sample size. This figure is applied to variable sampling formulas but not to attribute sampling formulas.

Key steps in the construction and selection of a sample for an audit test are seen in **figure 1.12**.

Sampling Risk

Sampling risk arises from the possibility that an IS auditor’s conclusion may be different from the conclusion that would be reached if the entire population were subjected to the same audit procedure. There are two types of sampling risk:

• **The risk of incorrect acceptance**—A material weakness is assessed as unlikely when, in fact, the population is materially misstated.

• **The risk of incorrect rejection**—A material weakness is assessed as likely when, in fact, the population is not materially misstated.

Note: A CISA candidate is not expected to be a sampling expert.

However, a CISA candidate should have a foundational understanding of the general principles of sampling and how to design a sample that is reliable. A CISA candidate should also be familiar with the different types of sampling terms and techniques and when it is appropriate to use each technique.

1.8 AUDIT EVIDENCE COLLECTION TECHNIQUES

Evidence is any information used by an IS auditor to determine whether the entity or data being audited follows the established criteria or objectives and supports audit conclusions. It is a requirement that conclusions be based on

sufficient, relevant and competent evidence. When planning the IS audit, the

type of audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability should be considered.

Audit evidence may include:

• An IS auditor's observations (presented to management)

• Notes taken from interviews

• Results of independent confirmations obtained by an IS auditor from different stakeholders

• Material extracted from correspondence and internal documentation or contracts with external partners

• The results of audit test procedures

While all evidence will assist an IS auditor in developing audit conclusions, some types of evidence are more reliable than others. The rules of evidence and sufficiency as well as the competency of evidence must be considered as required by audit standards.

Determinants for evaluating the reliability of audit evidence include:

• **Independence of the provider of the evidence**—Evidence obtained from outside sources is more reliable than from within the organization. This is why confirmation letters are used for verification of accounts receivable balances. Additionally, signed contracts or agreements with external parties could be considered reliable if the original documents are made available for review.

• **Qualifications of the individual providing the information/evidence**—

Whether the providers of the information/evidence are inside or outside of the organization, an IS auditor should always consider the qualifications and functional responsibilities of the persons providing the information.

This can also be true of an IS auditor. If an IS auditor does not have a good understanding of the technical area under review, the information gathered from testing that area may not be reliable, especially if the IS auditor does not fully understand the test.

Figure 1.12—Steps in the Selection of a Sample for an Audit Test



Source: ISACA, *Fundamentals of IS Audit and Assurance Training Course*, USA, 2014

• **Objectivity of the evidence**—Objective evidence is more reliable than evidence that requires considerable judgment or interpretation. An IS

auditor's review of media inventory is direct, objective evidence. An IS

auditor's analysis of the efficiency of an application, based on discussions with certain personnel, may not be objective audit evidence.

• **Timing of the evidence**—An IS auditor should consider the time during which information exists or is available in determining the nature, timing and extent of compliance testing and, if applicable, substantive testing. For example, audit evidence processed by dynamic systems, such as

spreadsheets, may not be retrievable after a specified period of time if changes to the files are not controlled or the files are not backed up.

An IS auditor gathers a variety of evidence during the audit. Some evidence may be relevant to the objectives of the audit, while other evidence may be considered peripheral. An IS auditor should focus on the overall objectives of the review and not the nature of the evidence gathered.

The quality and quantity of evidence must be assessed. These two characteristics are referred to by the International Federation of Accountants (IFAC) as competent (quality) and sufficient (quantity). Evidence is competent when it is both valid and relevant. Audit judgment is used to determine when sufficiency is achieved in the same manner that is used to determine the competency of evidence.

An understanding of the rules of evidence is important for IS auditors because they may encounter a variety of evidence types.

Note: A CISA candidate, given an audit scenario, should be able to determine which type of evidence-gathering technique would be best in a

given situation.

The following are techniques for gathering evidence:

• **Reviewing IS organization structures**—An organizational structure that provides an adequate separation or segregation of duties is a key general control in an IS environment. An IS auditor should understand general organizational controls and be able to evaluate these controls in the organization under audit. Where there is a strong emphasis on cooperative distributed processing or on end-user computing, IT functions may be organized somewhat differently from the classic IS organization, which consists of separate systems and operations functions. An IS audit and assurance should be able to review these organizational structures and assess the level of control they provide.

• **Reviewing IS policies and procedures**—An IS auditor should review whether appropriate policies and procedures are in place, determine whether personnel understand the implemented policies and procedures, and ensure that policies and procedures are being followed. An IS auditor should verify that management assumes full responsibility for formulating, developing, documenting, promulgating and controlling policies covering general aims and directives. Periodic reviews of policies and procedures for appropriateness should be carried out.

• **Reviewing IS standards**—An IS auditor should first understand the existing standards in place within the organization.

• **Reviewing IS documentation**—A first step in reviewing the documentation for an information system is to understand the existing documentation in place within the organization. This documentation could be a hard copy or stored electronically. If the latter is the case, controls to preserve the document integrity should be evaluated by an IS auditor. An IS auditor should look for a minimum level of IS documentation.

Documentation may include:

– Systems development initiating documents (e.g., feasibility study)

– Documentation provided by external application suppliers

– SLAs with external IT providers

– Functional requirements and design specifications

– Tests plans and reports

– Program and operations documents

– Program change logs and histories

– User manuals

– Operations manuals

– Security-related documents (e.g., security plans, risk assessments)

– BCPs

– QA reports

– Reports on security metrics

• **Interviewing appropriate personnel**—Interviewing techniques are an important skill for an IS auditor. Interviews should be organized in advance with objectives clearly communicated, follow a fixed outline and be documented by interview notes. An interview form or checklist prepared by an IS auditor is a good approach. Remember that the purpose of such an interview is to gather audit evidence using techniques such as inquiry, observation, inspection, confirmation, performance and monitoring.

Personnel interviews are discovery in nature and should never be accusatory; the interviewer should help people feel comfortable, encouraging them to share information, ideas, concerns and knowledge. An IS auditor should verify the accuracy of the notes with the interviewee.

• **Observing processes and employee performance**—The observation of processes is a key audit technique for many types of review. An IS auditor should be unobtrusive while making observations and should document

everything in sufficient detail to be able to present it, if required, as audit evidence. In some situations, the release of the audit report may not be timely enough to use this observation as evidence. This may necessitate the issuance of an interim report to management of the area being audited. An IS auditor may also wish to consider whether documentary evidence would be useful as evidence (e.g., photograph of a server room with doors fully opened).

• **Reperformance**—The reperformance process is a key audit technique that generally provides better evidence than the other techniques and is, therefore, used when a combination of inquiry, observation and

examination of evidence does not provide sufficient assurance that a control is operating effectively.

• **Walk-throughs**—The walk-through is an audit technique to confirm the understanding of controls.

While these evidence-gathering techniques are part of an audit, an audit is not considered only review work. It includes examination, which incorporates the testing of controls and audit evidence and, therefore, includes the results of audit tests.

An IS auditor should recognize that with systems development techniques such as computer-aided software engineering (CASE) or prototyping, traditional systems documentation will not be required or will be provided as an automated form. However, an IS auditor should look for documentation standards and practices within the IS organization.

An IS auditor should be able to review documentation for a given system and determine whether it follows the organization’s documentation standards. In addition, an IS auditor should understand the current approaches to developing systems such as object orientation, CASE tools or prototyping, and how the documentation is constructed. An IS auditor should recognize other components of IS documentation such as database specifications, file layouts or self-documented program listings.

1.8.1 INTERVIEWING AND OBSERVING PERSONNEL IN

PERFORMANCE OF THEIR DUTIES

Observing personnel in the performance of their duties assists an IS auditor in identifying:

• **Actual functions**—Observation could be an adequate test to ensure that the individual who is assigned and authorized to perform a particular function is the person who is actually doing the job. It allows an IS auditor an opportunity to witness how policies and procedures are understood and practiced. Depending on the specific situation, the results of this type of test should be compared with the respective logical access rights.

• **Actual processes/procedures**—Performing a walk-through of the process/procedure allows an IS auditor to obtain evidence of compliance and observe deviations, if any. This type of observation could prove to be useful for physical controls.

• **Security awareness**—Security awareness should be observed to verify an individual's understanding and practice of good preventive and detective

security measures to safeguard the enterprise's assets and data. This type of information could be supported with an examination of previous and planned security training.

• **Reporting relationships**—Reporting relationships should be observed to ensure that assigned responsibilities and adequate SoD are being practiced.

Often, the results of this type of test should be compared with the respective logical access rights.

• **Observation drawbacks**—The observer may interfere with the observed environment. Personnel, upon noticing that they are being observed, may change their usual behavior. Interviewing information processing personnel and management should provide adequate assurance that the staff has the required technical skills to perform the job. This is an important factor that contributes to an effective and efficient operation.

1.9 DATA ANALYTICS

Data analytics is an important tool for an IS auditor. Through the use of technology, an IS auditor can select and analyze full data sets to continuously audit or monitor key organizational data for abnormalities or variances that can

be used to identify and evaluate organizational risk and compliance with control and regulatory requirements. An IS auditor can use data analytics for the following purposes:

• Determination of the operational effectiveness of the current control environment

• Determination of the effectiveness of antifraud procedures and controls

• Identification of business process errors

• Identification of business process improvements and inefficiencies in the control environment

• Identification of exceptions or unusual business rules

• Identification of fraud

• Identification of areas where poor data quality exists

• Performance of risk assessment at the planning phase of an audit The process used to collect and analyze data includes the following elements:

• Setting the scope (e.g., determining audit/review objectives; defining data needs, sources and reliability)

• Identifying and obtaining the data (e.g., requesting data from responsible

sources, testing a sample of data, extracting the data for use)

• Validating the data (e.g., determining if the data are sufficient and reliable to perform audit tests) by:

– Validating balances independent of the data set extracted

– Reconciling detailed data to report control totals

– Validating numeric, character and date fields

– Verifying the time period of the data set (i.e., meets scope and purpose)

– Verifying that all necessary fields in scoping are actually included in the acquired data set

• Executing the tests (e.g., running scripts and performing other analytical tests)

• Documenting the results (e.g., recording the testing purpose, data sources and conclusions reached)

• Reviewing the results (e.g., ensuring that the testing procedures have been adequately performed and reviewed by a qualified person)

• Retaining the results (e.g., maintaining important test elements), such as:

– Program files

– Scripts

– Macros/automated command tests

– Data files

Data analytics can be effective for an IS auditor in both the planning and fieldwork phases of the audit. Data analytics can be used to accomplish the following:

• Combining logical access files with human resources employee master files for authorized users

• Combining file library settings with data from the change management systems and dates of file changes that can be matched to dates of authorized events

• Matching ingress with egress records to identify tailgating in physical security logs

• Reviewing table or system configuration settings

• Reviewing system logs for unauthorized access or unusual activities

• Testing system conversion

• Testing logical access SoD (e.g., analyzing Active Directory data combined

with job descriptions)

1.9.1 COMPUTER-ASSISTED AUDIT TECHNIQUES

CAATs are important tools that an IS auditor uses to gather and analyze data during an IS audit or review. When systems have different hardware and software environments, data structures, record formats or processing functions, it is almost impossible for an IS auditor to collect certain evidence without using such a software tool.

CAATs also enable an IS auditor to gather information independently. They provide a means to gain access and analyze data for a predetermined audit objective and to report the audit findings with emphasis on the reliability of the records produced and maintained in the system. The reliability of the source of the information used provides reassurance on findings generated.

CAATs include many types of tools and techniques such as generalized audit software (GAS), utility software, debugging and scanning software, test data, application software tracing and mapping, and expert systems.

GAS refers to standard software that has the capability to directly read and access data from various database platforms, flat-file systems and ASCII formats. GAS provides an IS auditor with an independent means to gain access to data for analysis and the ability to use high-level, problem-solving software to invoke functions to be performed on data files. Features include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and recomputations. The following functions are commonly supported by GAS:

• **File access**—Enables the reading of different record formats and file structures

• **File reorganization**—Enables indexing, sorting, merging and linking with another file

• **Data selection**—Enables global filtration conditions and selection criteria

• **Statistical functions**—Enables sampling, stratification and frequency analysis

• **Arithmetical function**s—Enables arithmetic operators and functions Utility software is a subset of software—such as report generators of the database

management system—that provides evidence about system control

effectiveness. Test data involve an IS auditor using a sample set of data to assess whether logic errors exist in a program and whether the program meets its objectives. The review of an application system will provide information about internal controls built in the system. The audit-expert system will give direction and valuable information to all levels of auditors while carrying out the audit because the query-based system is built on the knowledge base of senior auditors or managers.

These tools and techniques can be used in performing various audit procedures such as:

• Tests of the details of transactions and balances

• Analytical review procedures

• Compliance tests of IS general controls

• Compliance tests of IS application controls

• Network and OS vulnerability assessments

• Penetration testing

• Application security testing and source code security scans

An IS auditor should have a thorough understanding of CAATs and know where and when to apply them. For example, an IS auditor should review the results of engagement procedures to determine whether there are indications that irregularities or illegal acts may have occurred. Using CAATs could aid significantly in the effective and efficient detection of irregularities or illegal acts.

An IS auditor should weigh the costs and benefits of using CAATs before going through the effort, time and expense of purchasing or developing them.

Issues to consider include:

• Ease of use for existing and future audit staff

• Training requirements

• Complexity of coding and maintenance

• Flexibility of uses

• Installation requirements

• Processing efficiencies

• Effort required to bring the source data into the CAATs for analysis

• Ensuring the integrity of imported data by safeguarding their authenticity

• Recording the time stamp of data downloaded at critical processing points to sustain the credibility of the review

• Obtaining permission to install the software on the auditee servers

• Reliability of the software

• Confidentiality of the data being processed

When developing CAATs, the following are examples of documentation to be retained:

• Online reports detailing high-risk issues for review

• Commented program listings

• Flowcharts

• Sample reports

• Record and file layouts

• Field definitions

• Operating instructions

• Description of applicable source documents

CAATs documentation should be referenced to the audit program and clearly identify the audit procedures and objectives being served. When requesting access to production data for use with CAATs, an IS auditor should request read-only access. Any data manipulation by an IS auditor should be applied to copies of production files in a controlled environment to ensure that production data are not exposed to unauthorized updating. Most CAATs allow for production data to be downloaded from production systems to a stand-alone platform and then analyzed from the standalone platform, thereby insulating the production systems from any adverse impact.

CAATs as a Continuous Online Audit Approach

An important advantage of CAATs is the ability to improve audit efficiency through continuous online auditing techniques. To this end, an IS auditor must develop audit techniques that are appropriate for use with advanced information systems. In addition, they must be involved in the creation of advanced systems at the early stages of development and implementation and must make greater use of automated tools that are suitable for their organization's automated environment. This takes the form of the continuous audit approach.

1.9.2 CONTINUOUS AUDITING AND MONITORING

Continuous auditing is an approach used by IS auditors to monitor system reliability on a continuous basis and gather selective audit evidence through the computer. A distinctive characteristic of continuous auditing is the short time lapse between the facts to be audited, the collection of evidence and audit reporting. To properly understand the implications and requirements of continuous auditing, a distinction is made between continuous auditing and continuous monitoring:

• **Continuous auditing**—Enables an IS auditor to perform tests and assessments in a real-time or near-real-time environment. Continuous auditing is designed to enable an IS auditor to report results on the subject matter being audited within a much shorter time frame than under a traditional audit approach.

• **Continuous monitoring**—Used by an organization to observe the performance of one or many processes, systems or types of data. For example, real-time antivirus or IDSs may operate in a continuous monitoring fashion.

Continuous auditing should be independent of continuous control or monitoring

activities. When both continuous monitoring and auditing take place, continuous assurance can be established. In practice, continuous auditing is the precursor to management adopting continuous monitoring as a process on a day-to-day basis. Often, the audit function will hand over the techniques used in continuous auditing to the business, which will then run the continuous monitoring. This collaboration has led to increased appreciation among process owners of the value that the audit function brings to the organization, leading to greater confidence and trust between the business and the audit function. Nevertheless, the lack of independence and objectivity inherent in continuous monitoring should not be overlooked, and continuous monitoring should never be considered as a substitute for the audit function.

Continuous auditing efforts often incorporate new IT developments; increased processing capabilities of current hardware, software, standards and AI tools; and attempts to collect and analyze data at the moment of the transaction. Data must be gathered from different applications working within

different environments, transactions must be screened, the transaction environment has to be analyzed to detect trends and exceptions, and atypical patterns (i.e., a transaction with significantly higher or lower value than typical for a given business partner) must be exposed. If all this must happen in real time, perhaps even before final sign-off of a transaction, it is mandatory to adopt and combine various top-level IT techniques. The IT

environment is a natural enabler for the application of continuous auditing because of the intrinsic automated nature of its underlying processes.

Continuous auditing aims to provide a more secure platform to avoid fraud and a real-time process aimed at ensuring a high level of financial control.

Continuous auditing and monitoring tools are often built into many enterprise resource planning packages and most OS and network security packages.

These environments, if appropriately configured and populated with rules, parameters and formulas, can output exception lists on request while operating against actual data. Therefore, they represent an instance of continuous auditing. The difficulty, but significant added value, of using these features is that they postulate a definition of what would be a

“dangerous” or exception condition. For example, whether a set of granted IS

access permissions is to be deemed risk-free will depend on having well-defined SoD. On the other hand, it may be much harder to decide if a given sequence of steps taken to modify and maintain a database record points to a potential risk.

It is important to validate the source of the data used for continuous auditing and note the possibility of manual changes.

1.9.3 CONTINUOUS AUDITING TECHNIQUES

Continuous audit techniques are important IS audit tools, particularly when they are used in time-sharing environments that process a large number of transactions but leave a scarce paper trail. By permitting an IS auditor to evaluate operating controls on a continuous basis without disrupting the organization's usual operations, continuous audit techniques improve the security of a system. When a system is misused by someone withdrawing money from an inoperative account, a continuous audit technique will report this withdrawal in a timely fashion to an IS auditor. Thus, the time lag

between the misuse of the system and the detection of that misuse is reduced.

The realization that failures, improper manipulation and lack of controls will be detected on a timely basis by the use of continuous audit procedures gives an IS auditor and management greater confidence in a system's reliability.

There are five types of automated evaluation techniques applicable to continuous auditing:

1. **Systems control audit review file and embedded audit modules (SCARF/EAM)**—The use of this technique involves embedding specially written audit software in the organization's host application system so the application systems are monitored on a selective basis.

2. **Snapshots**—This technique involves taking what might be termed

"pictures" of the processing path that a transaction follows, from the input to the output stage. With the use of this technique, transactions are tagged by applying identifiers to input data and recording selected information about what occurs for an IS auditor's subsequent review.

3. **Audit hooks**—This technique involves embedding hooks in application

systems to function as red flags and induce IS security and auditors to act before an error or irregularity gets out of hand.

4. **Integrated test facility (ITF)**—In this technique, dummy entities are set up and included in an auditee's production files. An IS auditor can make the system either process live transactions or test transactions during regular processing runs and have these transactions update the records of the dummy entity. The operator enters the test transactions simultaneously with the live transactions that are entered for processing. An auditor then compares the output with the data that have been independently calculated to verify the correctness of the computer-processed data.

5. **Continuous and intermittent simulation (CIS)**—During a process run of a transaction, the computer system simulates the instruction execution of the application. As each transaction is entered, the simulator decides whether the transaction meets certain predetermined criteria and, if so, audits the transaction. If not, the simulator waits until it encounters the next transaction that meets the criteria.

In **figure 1.13,** the relative advantages and disadvantages of the various continuous audit tools are presented.

Figure 1.13—Continuous Audit Tools—Advantages and Disadvantages

	SCARF/EAM	Snapshots	Audit Hooks	ITF	CIS
Complexity	Very high	Medium	Low	High	Medium
Useful when:	Regular processing cannot be interrupted.	An audit trail is required.	Only select transactions or processes need to be examined.	It is not beneficial to use test data.	Transactions meeting certain criteria need to be examined.

The use of each of the continuous audit techniques has advantages and disadvantages. Their selection and implementation depends, to a large extent, on the complexity of an organization's computer systems and applications, and an IS auditor's ability to understand and evaluate the system with and without the use of continuous audit techniques. In addition, an IS auditor must recognize that continuous audit techniques are not a cure for all control problems and the use of these techniques provides only limited assurance that the information processing systems examined are operating as they were intended to function.

Techniques that are used to operate in a continuous auditing environment must work at all data levels—single input, transaction and databases—and include:

• Transaction logging

• Query tools

• Statistics and data analysis

• DBMS

• Data warehouses, data marts, data mining

• Intelligent agents

• EAM

• Neural network technology

• Standards such as Extensible Business Reporting Language (XBRL) Intelligent software agents may be used to automate the evaluation processes and allow for flexibility and dynamic analysis capabilities. The configuration and application of intelligent agents (sometimes referred to as bots) allow for continuous monitoring of systems settings and the delivery of alert messages when certain thresholds are exceeded or certain conditions are met.

Full continuous auditing processes have to be carefully built into applications and work in layers. The auditing tools must operate in parallel to normal

processing—capturing real-time data, extracting standardized profiles or descriptors, and passing the result to the auditing layers.

Continuous auditing has an intrinsic edge over point-in-time or periodic auditing because it captures internal control problems as they occur, preventing negative effects. Implementation can also reduce possible or intrinsic audit inefficiencies such as delays, planning time, inefficiencies of the audit process, overhead due to work segmentation, multiple quality or supervisory reviews, or discussions concerning the validity of findings.

Full top management support, dedication, and extensive experience and technical knowledge are all necessary to accomplish continuous auditing, while minimizing the impact on the underlying audited business processes.

The auditing layers and settings may also need continual adjustment and updating.

Besides difficulty and cost, continuous auditing has an inherent disadvantage in that internal control experts and auditors might be resistant to trust an automated tool in lieu of their personal judgment and evaluation. Also, mechanisms have to be put in place to eliminate false negatives and false positives in the reports generated by such audits so that the report generated continues to inspire stakeholders' confidence in its accuracy.

1.10 REPORTING AND COMMUNICATION TECHNIQUES

Effective and clear communication can significantly improve the quality of audits and maximize their results. Audit findings should be reported and communicated to stakeholders, with appropriate buy-in from the auditees, for the audit process to be successful. An IS auditor should also consider the motivations and perspectives of the recipients of the audit report so their concerns may be properly addressed. Communication skills (both written and verbal) determine the effectiveness of the audit reporting process.

Communication and negotiation skills are required throughout the audit.

Successful resolution of audit findings with auditees is essential so that auditees will adopt the recommendations in the report and initiate prompt corrective action. To achieve this goal, an IS auditor should be skilled in the

use of techniques such as facilitation, negotiation and conflict resolution. An IS auditor should also understand the concept of materiality (i.e., the relative importance of audit findings based on business impact) when reporting on audit results.

1.10.1 COMMUNICATING AUDIT RESULTS

The exit interview, conducted at the end of the audit, provides an IS auditor with the opportunity to discuss findings and recommendations with the auditee management. During the exit interview, an IS auditor should:

• Ensure that the facts presented in the report are correct and material.

• Ensure that the recommendations are realistic and cost-effective and, if not,

seek alternatives through negotiation with auditee management.

• Recommend implementation dates for agreed-on recommendations.

IS auditors should be aware that, ultimately, they are responsible to senior management and the audit committee and they should feel free to

communicate issues or concerns to these groups. An attempt to deny access by levels lower than senior management would limit the independence of the audit function.

Before communicating the results of an audit to senior management, an IS

auditor should discuss the findings with the auditee management to gain agreement on the findings and develop an agreed-upon course of corrective action. In cases where there is disagreement, an IS auditor should elaborate on the significance of the findings, risk and effects of not correcting the control weakness. Sometimes the auditee management may request assistance from an IS auditor in implementing the recommended control enhancements.

An IS auditor should communicate the difference between an IS auditor's role and that of a consultant and consider how assisting the auditee may adversely affect an IS auditor's independence.

After agreement has been reached with auditee management, IS audit management should brief senior auditee management. A summary of audit activities should be presented periodically to the audit committee. Audit committees typically are composed of individuals who do not work directly for the organization and, thus, provide an IS audit and assurance professional

with an independent route to report sensitive findings.

1.10.2 AUDIT REPORT OBJECTIVES

The six objectives of audit reporting are:

• Formally present the audit results to the auditee (and the audit client, if different from the auditee).

• Serve as formal closure of the audit engagement.

• Provide statements of assurance and, if needed, identification of areas requiring corrective action and related recommendations.

• Serve as a valued reference for any party researching the auditee or audit topic.

• Serve as the basis for a follow-up audit if audit findings were presented.

• Promote audit credibility. This depends on the report being well developed and well written.

The IS audit-specific reporting objectives are developed based on report requirements from auditee management and other users of the report and in compliance with IS audit and assurance standards and audit organization protocols. The auditee or other stakeholders, such as oversight organizations, are identified during audit planning. An IS auditor develops the audit scope and objectives by considering these requirements and other elements of audit planning, such as the assessments of risk, materiality, and appropriateness of stated controls together with regulatory and IT governance requirements. The audit report formally presents the purpose and the results of the audit in line with these requirements. Every audit report should provide unbiased, well-supported responses to the audit's objectives. For example, if the audit objective is to determine whether adequate controls are in effect to provide reasonable assurance that only authorized physical access can be gained to the data center, then the report should state an IS auditor's conclusion or opinion as to the adequacy of the controls to achieve that objective. If controls need to be implemented or strengthened to achieve the objective, then the report should provide a recommendation to meet that need.

1.10.3 AUDIT REPORT STRUCTURE AND CONTENTS

Audit reports are the end product of the IS audit work. The exact format of an

audit report will vary by organization; however, an IS auditor should understand the basic components of an audit report and how it communicates audit findings to management.

Note: The CISA candidate should become familiar with the ISACA IS

Audit and Assurance Standards 1401 Reporting and 1402 Follow-up

Activities.

Audit reports usually have the following structure and content:

• An introduction to the report, including a statement of audit objectives, limitations to the audit and scope, the period of audit coverage, and a general statement on the nature and extent of audit procedures conducted and processes examined during the audit, followed by a statement on the IS

audit methodology and guidelines

• Audit findings included in separate sections and often grouped in sections by materiality and/or intended recipient

• An IS auditor's overall conclusion and opinion on the adequacy of controls and procedures examined during the audit, and the actual potential risk identified as a consequence of detected deficiencies

• An IS auditor's reservations or qualifications with respect to the audit

– This may state that the controls or procedures examined were found to be adequate or inadequate. The balance of the audit report should support that conclusion, and the overall evidence gathered during the audit should provide an even greater level of support for the audit conclusions.

• Detailed audit findings and recommendations

– An IS auditor decides whether to include specific findings in an audit report. This should be based on the materiality of the findings and the intended recipient of the audit report. An audit report directed to the audit committee of the board of directors, for example, may not include findings that are important only to local management but have little control significance to the overall organization. The decision on what to include in various levels of audit reports depends on the guidance provided by upper management.

• A variety of findings, some of which may be quite material while others are

minor in nature

– An IS auditor may choose to present minor findings to management in an

alternate format, such as by memorandum.

An IS auditor should make the final decision about what to include or exclude from the audit report. Generally, an IS auditor should be concerned with providing a balanced report, describing not only negative issues in terms of findings but positive constructive comments regarding improved processes and controls or effective controls already in place. Overall, an IS auditor should exercise independence in the reporting process.

Auditee management evaluates the findings, stating corrective actions to be taken and timing for implementing these anticipated corrective actions.

Management may not be able to implement all audit recommendations immediately. For example, an IS auditor may recommend changes to an information system that is also undergoing other changes or enhancements.

An IS auditor should not necessarily expect that the other changes will be suspended until their recommendations are implemented. Rather, all may be implemented at once.

An IS auditor should discuss the recommendations and any planned implementation dates while in the process of releasing the audit report.

Various constraints—such as staff limitations, budgets or other projects—

may limit immediate implementation. Management should develop a firm program for corrective actions. It is important to obtain a commitment from auditee management on the date by which the action plan will be

implemented (the solution can take a long time for implementation) and the manner in which it will be performed because the corrective action may bring risk that may be avoided if identified while discussing and finalizing the audit report. If appropriate, an IS auditor may want to report to senior management on the progress of implementing recommendations.

The report should include all significant audit findings. When a finding requires explanation, an IS auditor should describe the finding, its cause and risk. When appropriate, an IS auditor should provide the explanation in a separate document and refer to it in the report. For example, this approach

may be appropriate for highly confidential matters. An IS auditor should also identify the organizational, professional and governmental criteria applied.

The report should be issued in a timely manner to encourage prompt corrective action. When appropriate, an IS auditor should promptly communicate significant findings to the appropriate persons prior to the issuance of the report. Prior communication of significant findings should not alter the intent or content of the report.

1.10.4 AUDIT DOCUMENTATION

Audit documentation is the written record that provides the support for the representations in the auditor's report. It should:

1. Demonstrate that the engagement complied with the standards.

2. Support the basis for the auditor's conclusions.

Audit documentation should include, at a minimum, a record of the following:

• Planning and preparation of the audit scope and objectives

• Description and/or walk-throughs on the scoped audit area

• Audit program

• Audit steps performed and audit evidence gathered

• Use of services of other auditors and experts

• Audit findings, conclusions and recommendations

• Audit documentation relation with document identification and dates It is also recommended that documentation include these items:

• A copy of the report issued as a result of the audit work

• Evidence of audit supervisory review

Documents should include audit information that is required by laws and regulations, contractual stipulations, and professional standards. Audit

documentation is the necessary evidence supporting the conclusions reached and should be clear, complete, easily retrievable and sufficiently comprehensible. Audit documentation is generally the property of the auditee and should be accessible only to authorized personnel under specific or general permission. When access to audit documentation is requested by external parties, an IS audit and assurance professional should obtain

appropriate prior approval of senior management and legal counsel before providing it to those external parties.

Policies should be developed regarding custody, retention requirements and release of audit documentation. The documentation format and media are optional, but due diligence and good practices require that work papers be dated, initialed, page-numbered, relevant, complete, clear, self-contained and properly labeled, filed, and kept in custody. Work papers may be automated.

An IS auditor should consider how to maintain integrity and protection of audit test evidence to preserve its proof value in support of audit results.

An IS auditor should be able to prepare adequate work papers, narratives, questionnaires and understandable system flowcharts. Audit documentation or work papers can be considered the bridge or interface between the audit objectives and the final report. They should provide a seamless transition—

with traceability and accountability—from objectives to report and from report to objectives. The audit report, in this context, can be viewed as a set of particular work papers.

The quest for integrating work papers in the auditor’s eenvironment has resulted in all major audit and project management packages, CAATs, and expert systems offering a complete array of automated documentation and import-export features.

Audit documentation should support the findings and conclusions/opinions.

Time of evidence can be crucial to supporting audit findings and conclusions.

An IS auditor should take care to ensure that the evidence gathered and documented will be able to support audit findings and conclusions.

The concept of materiality is a key issue when deciding which findings to bring forward in an audit report. Key to determining the materiality of audit findings is the assessment of what would be significant to different levels of management. Assessment requires judging the potential effect of the finding if corrective action is not taken. The following are examples:

• A weakness in information security physical access controls at a remote distributed computer site may be significant to management at the site but

will not necessarily be material to upper management at headquarters.

However, there may be other matters at the remote site that would be material to upper management.

• A review of access deprovisioning discovers that a terminated user's access was not removed after the user's termination date, but it was caught during management's review of security access, at which time the terminated user's access was removed. This type of discovery would not likely be brought to the attention of upper management but would be documented and discussed with auditee management.

1.10.5 FOLLOW-UP ACTIVITIES

Auditing is an ongoing process. An IS auditor is not effective if audits are performed and reports issued, but no follow-up is conducted to determine whether management has taken appropriate corrective actions. IS auditors should have a follow-up program to determine if agreed-on corrective actions have been implemented. Although IS auditors who work for external audit firms may not necessarily follow this process, they may achieve these tasks if agreed to by the auditee.

The timing of the follow-up will depend on the criticality of the findings and is subject to an IS auditor's judgment. The results of the follow-up should be communicated to appropriate levels of management. The level of an IS

auditor's follow-up review will depend on several factors. In some instances, an IS auditor may merely need to inquire as to the current status. In other instances, an IS auditor who works in an internal audit function may have to perform certain audit steps to determine whether the corrective actions agreed on by management have been implemented.

1.10.6 TYPES OF IS AUDIT REPORTS

The IS audit report is driven mainly by the type of audit engagement and the reporting requirements from IS audit and assurance standards. While most IS

audits result in a single IS audit report, in some situations, more than one report can be applicable. For example, in addition to a report for a general audience, a separate confidential security report containing detailed technical information may need to be created to ensure that security risk is not made

available to unintended parties.

The organization and specific content of the report also depend on the scope and objectives of the audit engagement and the degree to which IT processes and systems are examined or require explanation. The format and protocols for audit report presentation can also depend on any requirements and expectations set forth between the audit organization and the auditee.

Requirements for audit report contents or format may be requested by the audit client who may or may not be from the organization as the auditee.

Although review, examination and agreed-upon procedure engagements have similar reporting requirements, each type of engagement stipulates different reporting requirements and limitations. The primary distinctions among reviews, examinations and agreed-upon procedures engagements are the audit objectives, the nature and extent of audit work, and the level of assurance to be provided. While all three types of audits include review work, performing audit tests is far more prevalent in audits or examinations that require stronger evidence upon which to base an opinion. Agreed-upon procedures may also include testing, but because of other limitations, an audit opinion is not expressed. Although audit scope may be the same for reviews and examinations, scope is likely to be more narrowly defined for agreed-upon procedure audits.

1.11 QUALITY ASSURANCE AND IMPROVEMENT OF

THE AUDIT PROCESS

An IS auditor plays an important role in improving the quality and control of information systems in an organization. Elements of quality control with respect to an audit engagement include the following:

• Leadership responsibilities for quality in audits

• Ethical requirements (including independence)

• Acceptance and continuance of client relationships and specific audit engagements

• Assignment of engagement teams

• Engagement performance (including consultation, resolution of differences of opinion and engagement quality control review)

• Monitoring

Quality assurance is often achieved by the IS auditor serving as a consultant, advising and facilitating business areas to participate in process improvement and control. One such approach is through the process of control self-assessment (CSA).

1.11.1 CONTROL SELF-ASSESSMENT

CSA is an assessment of controls made by the staff and management of the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal control system of the organization is reliable. It also ensures that employees are aware of the risk to the business and they conduct periodic, proactive reviews of controls. It is a methodology used to review key business objectives; risk involved in achieving the business objectives; and internal controls designed to manage business risk in a formal, documented and collaborative process.

An IS auditor acts in the role of facilitator to the business process owners to help them define and assess appropriate controls and helps the process owners understand the need for controls, based on risk to the business processes. The process owners and the personnel who run the processes use their knowledge and understanding of the business function to evaluate the performance of controls against the established control objectives, while considering the risk appetite of the organization. Process owners are in an ideal position to define the appropriate controls because they have a greater knowledge of the process objectives.

A CSA program can be implemented by various methods. For small business units within organizations, it can be implemented by facilitated workshops in which functional management and IS auditors come together and deliberate how best to evolve a control structure for the business unit. In a workshop, the role of a facilitator is to support the decision-making process. The facilitator creates a supportive environment to help participants explore their own experiences and those of others; identify control strengths and weaknesses; and share their knowledge, ideas and concerns. If appropriate, a facilitator may also offer his/her own expertise in addition to facilitating the

exchange of ideas and experience.

Objectives of CSA

The primary objective of a CSA program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional areas. It is not intended to replace audit's responsibilities but to enhance them. Auditees such as line managers are responsible for controls in their environment; the managers should also be responsible for monitoring the controls. CSA programs must also educate management about control design and monitoring, particularly concentrating on areas of high risk.

When employing a CSA program, measures of success for each phase (planning, implementation and monitoring) should be developed to determine the value derived from CSA and its future use. One critical success factor (CSF) is to conduct a meeting with the business unit representatives (including appropriate and relevant staff and management) to identify the business unit's primary objective—to determine the reliability of the internal control system. In addition, actions that increase the likelihood of achieving the primary objective should be identified.

Benefits of CSA

Some of the benefits of CSA include the following:

• Early detection of risk

• More effective and improved internal controls

• Creation of cohesive teams through employee involvement

• Development of a sense of ownership of the controls in the employees and process owners and reduction of their resistance to control improvement initiatives

• Increased employee awareness of organizational objectives, and knowledge of risk and internal controls

• Increased communication between operational and top management

• Highly motivated employees

• Improved audit rating process

• Reduction in control cost

• Assurance provided to stakeholders and customers

• Necessary assurance given to top management about the adequacy of

internal controls as required by the various regulatory agencies and laws

Disadvantages of CSA

CSA contains some disadvantages, including:

• It could be mistaken as an audit function replacement.

• It may be regarded as an additional workload (e.g., one more report to be submitted to management).

• Failure to act on improvement suggestions could damage employee morale.

• Lack of motivation may limit effectiveness in the detection of weak controls.

The IS Auditor's Role in CSA

When CSA programs are established, auditors become internal control professionals and assessment facilitators. Their value in this role is evident when management takes responsibility and ownership for internal control systems under their authority through process improvements in their control structures, including an active monitoring component.

To be effective in this facilitative and innovative role, the IS auditor must understand the business process being assessed. It is important to remember that IS auditors are the facilitators and the management client is the participant in the CSA process. For example, during a CSA workshop, instead of performing detailed audit procedures, the IS auditor will lead and guide the auditees in assessing their environment by providing insight about the objectives of controls based on risk assessment. The managers, with a focus on improving the productivity of the process, might suggest replacement of preventive controls. In this case, the IS auditor is better positioned to explain the risk associated with such changes.

To provide higher-quality audits and make use of internal and/or external audit or subject matter expertise, an integrated audit approach is used to perform risk-based assessments of internal controls over an operation, process or entity.

1.11.2 INTEGRATED AUDITING

The dependence of business processes on IT has necessitated that all auditors

develop an understanding of IT control structures. In addition, IS auditors must develop an understanding of the business control structures. This type of integrated auditing can be defined as the process whereby appropriate audit disciplines are combined to assess key internal controls over an operation, process or entity and focuses on risk. A risk assessment aims to understand and identify risk arising from the entity and its environment, including relevant internal controls. At this stage, the role of an IS auditor is typically to understand and identify risk under topical areas such as information management, IT infrastructure, IT governance and IT operations.

Other audit and assurance specialists will seek to understand the organizational environment, business risk and business controls. A key element of the integrated approach is a discussion among the whole audit team of emerging risk, with consideration of impact and likelihood.

Detailed audit work focuses on the relevant controls in place to manage this risk. IT systems frequently provide a first line of preventive and detective controls, and the integrated audit approach depends on a sound assessment of their efficiency and effectiveness.

The integrated audit process typically involves the following elements:

• Identification of risk faced by the organization for the area being audited

• Identification of relevant key controls

• Review and understanding of the design of key controls

• Testing that key controls are supported by the IT system

• Testing that management controls operate effectively

• A combined report or opinion on control risk, design and weaknesses An integrated audit demands a focus on business risk and a drive for creative control solutions. It is a team effort of audit and assurance professionals with different skill sets. Using this approach permits a single audit of an entity with one comprehensive report. An additional benefit is that this approach assists in staff development and retention by providing greater variety and the ability to see how all of the elements (functional and IT) mesh together to form the complete picture. See **figure 1.14** for an integrated auditing approach.

Figure 1.14—An Integrated Audit



The integrated audit concept has also radically changed the way audits are accepted and valued by different stakeholders. For example:

• Employees or process owners better understand the objectives of an audit because they can see the linkage between controls and audit procedures.

• Top management better understands the linkage between increased control effectiveness and corresponding improvements in the allocation and utilization of IT resources.

• Shareholders better understand the linkage between the push for a greater

degree of corporate governance and its impact on the generation of financial statements that can be relied on.

All these developments have led to greater impetus for the growing popularity of integrated audits.

Note: A CISA candidate should be familiar with the integrated audit process and steps.

CASE STUDY

Betatronics is a mid-sized manufacturer of electronic goods with headquarters in the United States and factories located in Latin America. An IS auditor within the enterprise has been asked to perform preliminary work that will assess the organization's readiness for a review to measure compliance with new US-based regulatory requirements.

These requirements are designed to ensure that management is taking an active role in setting up and maintaining a well-controlled environment and will assess management's review and testing of the general IT controls. Areas to be assessed include:

• Logical and physical security

• Change management

• Production control and network management

• IT governance

• End-user computing

The IS auditor has been given six months to perform this preliminary work.

In previous years, repeated problems have been identified in the areas of logical security and change management. Logical security deficiencies noted included the sharing of administrator accounts and failure to enforce adequate controls over passwords. Change management deficiencies included improper segregation of incompatible duties and failure to document all changes. Additionally, the process for deploying operating system updates to servers was

found to be only partially effective.

In anticipation of the work to be performed by the IS auditor, the chief information officer (CIO) requested direct reports to develop narratives and process flows describing the major activities for which IT is responsible.

These were completed, approved by the various process owners and the CIO, and then forwarded to the IS auditor for examination.

1.

What should the IS auditor do **FIRST**?

A. Perform a survey audit of logical access controls.

B. Revise the audit plan to focus on risk-based auditing.

C. Perform an IT risk assessment.

D. Begin testing controls that the IS auditor feels are most critical.

2.

When auditing the logical security, the IS auditor is **MOST** concerned when observing:

A. The system administrator account is known by everybody.

B. The passwords are not enforced to change frequently.

C. The network administrator is given excessive permissions.

D. The IT department does not have written policy on privilege

management.

3.

When testing program change management in this case, how should the sample be selected?

A. Change management documents should be selected at random and

examined for appropriateness.

B. Changes to production code should be sampled and traced to

appropriate authorizing documentation.

C. Change management documents should be selected based on

system criticality and examined for appropriateness.

D. Changes to production code should be sampled and traced back to system-produced logs indicating the date and time of the change.

4.

List three general IT controls the IS auditor would use for substantive testing in this case.

After the preliminary work has been completed, Betatronics decides to plan audits for the next two years. After accepting the appointment, the IS auditor notes that:

• The entity has an audit charter that details the scope and responsibilities of the IS audit function and specifies the audit committee as the overseeing body for audit activity.

• The entity is subject to regulatory compliance requirements that require its

management to certify the effectiveness of the internal control system as it relates to financial reporting.

• The entity has been recording consistent growth over the last two years at double the industry average.

• The entity has seen increased employee turnover as well.

5.

The **FIRST** priority of the IS auditor in year one should be to study the:

A. previous IS audit reports and plan the audit schedule.

B. audit charter and plan the audit schedule.

C. impact of the increased employee turnover.

D. impact of the implementation of a new ERP on the IT environment.

6.

How should the IS auditor evaluate backup and batch processing within computer operations?

A. Rely on the service auditor’s report of the service provider.

B. Study the contract between the entity and the service provider.

C. Compare the service delivery report to the service level agreement.

D. Plan and carry out an independent review of computer operations.

7.

During the day-to-day work, the IS auditor advises there is a risk that log review may not result in timely detection of errors. This is an example of which of the following:

A. inherent risk

B. residual risk

C. control risk

D. material risk

8.

The IS auditor advised the CIO and team to improve the general IT

control environment. COBIT was proposed to be adapted. What

recommendations would the IS auditor make when considering this

framework?

ANSWERS TO CASE STUDY QUESTIONS

1.

A.

Performing a survey audit of logical access controls would occur after an IT risk assessment.

B.

Revising the audit plan to focus on risk-based auditing would

occur after an IT risk assessment.

C.

An IT risk assessment should be performed first to ascertain

which areas present the greatest risk and what controls

mitigate that risk. Although narratives and process flows

have been created, the organization has not yet assessed

which controls are critical.

D.

Testing controls that the IS auditor feels are most critical would occur after an IT risk assessment.

2.

A.

The system administrator account being known by

everybody is most dangerous. In that case, any user could perform any action in the system, including file access, permission and parameter adjustment.

B.

Infrequent password changing would present a concern but would not be a serious as everyone knowing the system administrator account.

C.

The network administrator being given excessive permissions would present a concern, but it would not be as serious as everyone knowing the system administrator account.

D.

The absence of a privilege management policy would be a concern, but it would not be as serious as everyone knowing the system administrator account.

3.

A.

When a sample is chosen from a set of control documents, there is no way to ensure that every change was accompanied by appropriate control documentation.

B.

When testing a control, it is advisable to trace from the item being controlled to the relevant control documentation. When

a sample is chosen from a set of control documents, there is

no way to ensure that every change was accompanied by

appropriate control documentation. Accordingly, changes to

production code provide the most appropriate basis for selecting a sample.

C.

When a sample is chosen from a set of control documents, there

is no way to ensure that every change was accompanied by

appropriate control documentation.

D.

When testing a control, it is advisable to trace from the item

being controlled to the relevant control documentation.

4.

Some possible answers include:

• The IS auditor can check which account was used for executing a particular system administrator task recently.

• The IS auditor can check if there was a change record for any

selected system changes (i.e., server reboot and patching).

• The IS auditor can look into the transactions to see if they separated the incompatible duties.

5.

A.

Previous IS audit reports will be revisited to save redundant work and for reference when doing the particular IS audit work.

B.

The audit charter defines the purpose, authority and

responsibility of the IS audit activities. It also sets the

foundation for upcoming activities.

C.

Impact of employee turnover would be addressed when

negotiating the follow-up activities on respective areas if there is any gap to close.

D.

Impact of the implementation of a new ERP would be addressed

when negotiating the follow-up activities on respective areas if there is any gap to close.

6.

A.

The service auditor’s report cannot assure the discovery of

control inefficiencies.

B.

Review of the contract cannot assure the discovery of control

inefficiencies.

C.

Comparing the service delivery report and the service level

agreement cannot assure the discovery of control inefficiencies.

D.

IS audit should conduct an independent review of the backup

and batch processing. All other choices cannot assure the

discovery of control inefficiencies in the process.

7.

A.

This is not an example of inherent risk. Inherent risk is the risk level or exposure without considering the actions that

management has taken or might take (e.g., implementing

controls).

B.

This is not an example of residual risk. Residual risk is the

remaining risk after management has implemented a risk

response.

C.

Control risk exists when a risk cannot be prevented or

detected on a timely basis by the system of IS controls, which is what is described in this instance.

D.

This is not an example of material risk. Material risk is any risk large enough to threaten the overall success of the business in a material way.

8.

Possible answer: The COBIT framework can be leveraged and adapted.

Each process can be classified as fully addressed, partially addressed and not applicable by comparing the standard COBIT framework to the organization's reality. Further frameworks, standards and practices can be included in each respective process, as COBIT guidance suggests.

Chapter 2:

Governance and Management of IT

Overview

Domain 2 Exam Content Outline

Learning Objectives/Task Statements

Suggested Resources for Further Study

Self-assessment Questions

Answers to Self-assessment Questions

Part A: IT Governance

2.0

Introduction

2.1

IT Governance and IT Strategy

2.2

IT-related Frameworks

2.3

IT Standards, Policies and Procedures

2.4

Organizational Structure

2.5

Enterprise Architecture

2.6

Enterprise Risk Management

2.7

Maturity Models

2.8

Laws, Regulations and Industry Standards Affecting the

Organization

Part B: IT Management

2.9

IT Resource Management

2.10 IT Service Provider Acquisition and Management

2.11 IT Performance Monitoring and Reporting 2.12 Quality Assurance and Quality Management of IT

Case Study

Case Study

Answers to Case Study Questions

OVERVIEW

Governance and management of IT are integral parts of enterprise governance. Effective governance and management of IT consist of the leadership and organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategy and objectives.

Knowledge of IT governance is fundamental to the work of the IS auditor, and it forms the foundation for the development of sound control practices and mechanisms for management oversight and review.

This domain represents 17 percent of the CISA examination (approximately 26 questions).

DOMAIN 2 EXAM CONTENT OUTLINE

Part A: IT Governance

1. IT Governance and IT Strategy

2. IT-related Frameworks

3. IT Standards, Policies, and Procedures

4. Organizational Structure

5. Enterprise Architecture

6. Enterprise Risk Management

7. Maturity Models

8. Laws, Regulations and Industry Standards Affecting the Organization **Part B. IT Management**

1. IT Resource Management

2. IT Service Provider Acquisition and Management

3. IT Performance Monitoring and Reporting

4. Quality Assurance and Quality Management of IT

LEARNING OBJECTIVES/TASK STATEMENTS

Within this domain, the IS auditor should be able to:

• Evaluate the IT strategy for alignment with the organization's strategies and objectives. (T5)

• Evaluate the effectiveness of IT governance structure and IT organizational structure. (T6)

• Evaluate the organization's management of IT policies and practices. (T7)

• Evaluate the organization's IT policies and practices for compliance with regulatory and legal requirements. (T8)

• Evaluate IT resource and portfolio management for alignment with the organization's strategies and objectives. (T9)

• Evaluate the organization's risk management policies and practices. (T10)

• Evaluate IT management and monitoring of controls. (T11)

• Evaluate the monitoring and reporting of IT key performance indicators (KPIs). (T12)

• Evaluate whether IT supplier selection and contract management processes align with business requirements. (T15)

• Evaluate whether IT service management practices align with business requirements. (T20)

• Conduct periodic review of information systems and enterprise

architecture. (T21)

• Evaluate data governance policies and practices. (T25)

• Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives. (T34)

• Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices. (T39)

SUGGESTED RESOURCES FOR FURTHER STUDY

Hales, Andrew; *The Definitive Handbook of Business Continuity Management, 3rd Edition*, John Wiley & Sons Inc., USA, 2011

International Organization for Standardization (ISO), *ISO/IEC 38500:2015: Information technology—Governance of IT for the Organization*, Switzerland, 2015

ISACA, *COBIT 2019*, USA, 2018, *www.isaca.org/cobit*

ISACA, *Getting Started with Governance of Enterprise IT (GEIT)*, USA,

2015, *http://www.isaca.org/Knowledge-*

Center/Research/ResearchDeliverables/Pages/getting-started-with-

governance-of-enterprise-it.aspx

ISACA, *Getting Started with GEIT: A Primer for Implementing Governance of Enterprise IT*, USA, 2016

ISACA, *The Risk IT Framework*, USA, 2011

ISACA, White papers, *http://www.isaca.org/Knowledge-*

Center/Research/Pages/White-Papers.aspx

SELF-ASSESSMENT QUESTIONS

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often, a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided. Please note that these questions are not actual or retired exam items. Please see the section

“About This Manual” at the beginning of this manual for more guidance regarding practice questions.

2-1

In order for management to effectively monitor the compliance of processes and applications, which of the following would be the **MOST**

ideal?

A. A central document repository

B. A knowledge management system

C. A dashboard

D. Benchmarking

2-2

Which of the following would be included in an IS strategic plan?

A. Specifications for planned hardware purchases B. Analysis of future business objectives

C. Target dates for development projects

D. Annual budgetary targets for the IT department

2-3

Which of the following **BEST** describes an IT department’s strategic planning process?

A. The IT department will have either short- or long-range plans depending on the organization’s broader plans and objectives.

B. The IT department’s strategic plan must be time- and project-

oriented but not so detailed as to address and help determine

priorities to meet business needs.

C. Long-range planning for the IT department should recognize

organizational goals, technological advances and regulatory

requirements.

D. Short-range planning for the IT department does not need to be integrated into the short-range plans of the organization since

technological advances will drive the IT department plans much

quicker than organizational plans.

2-4

The **MOST** important responsibility of a data security officer in an organization is:

A. recommending and monitoring data security policies.

B. promoting security awareness within the organization.

C. establishing procedures for IT security policies.

D. administering physical and logical access controls.

2-5

What is considered the **MOST** critical element for the successful implementation of an information security program?

A. An effective enterprise risk management framework

B. Senior management commitment

C. An adequate budgeting process

D. Meticulous program planning

2-6

An IS auditor should ensure that IT governance performance measures: A. evaluate the activities of IT oversight committees.

B. provide strategic IT drivers.

C. adhere to regulatory reporting standards and definitions.

D. evaluate the IT department.

2-7

Which of the following tasks may be performed by the same person in a well-controlled information processing computer center?

A. Security administration and change management

B. Computer operations and system development

C. System development and change management

D. System development and system maintenance

2-8

Which of the following is the **MOST** critical control over database administration (DBA)?

A. Approval of DBA activities

B. Segregation of duties in regard to access rights granting/revoking C. Review of access logs and activities

D. Review of the use of database tools

2-9

When a complete segregation of duties cannot be achieved in an online system environment, which of the following functions should be

separated from the others?

A. Origination

B. Authorization

C. Recording

D. Correction

2-10 In a small organization where segregation of duties (SoD) is not practical, an employee performs the function of computer operator and application programmer. Which of the following controls should the IS

auditor recommend?

A. Automated logging of changes to development libraries

B. Additional staff to provide SoD

C. Procedures that verify that only approved program changes are implemented

D. Access controls to prevent the operator from making program

modifications

ANSWERS TO SELF-ASSESSMENT QUESTIONS

2-1

A.

A central document repository provides a great deal of data but

not necessarily the specific information that would be useful for monitoring and compliance.

B.

A knowledge management system provides valuable information

but is generally not used by management for compliance

purposes.

C.

A dashboard provides a set of information to illustrate

compliance of the processes, applications and configurable

elements and keeps the enterprise on course.

D.

Benchmarking provides information to help management adapt

the organization, in a timely manner, according to trends and

environment.

2-2

A.

Specifications for planned hardware purchases are not strategic

items.

B.

IS strategic plans must address the needs of the business and meet future business objectives. Hardware purchases may be

outlined, but not specified, and neither budget targets nor

development projects are relevant choices.

C.

Target dates for development projects are not strategic items.

D.

Annual budgetary targets for the IT department are not strategic items.

2-3

A.

Typically, the IT department will have short- or long-range plans that are consistent and integrated with the organization’s plans.

B.

These plans must be time- and project-oriented and address the

organization’s broader plans toward attaining its goals.

C.

Long-range planning for the IT department should recognize

organizational goals, technological advances and regulatory

requirements.

D.

Short-range planning for the IT department should be integrated

into the short-range plans of the organization to better enable the IT department to be agile and responsive to needed technological advances that align with organizational goals and objectives.

2-4

A.

A data security officer’s prime responsibility is

recommending and monitoring data security policies.

B.

Promoting security awareness within the organization is one of

the responsibilities of a data security officer, but it is not as important as recommending and monitoring data security

policies.

C.

The IT department, not the data security officer, is responsible for establishing procedures for IT security policies recommended by

the data security officer.

D.

The IT department, not the data security officer, is responsible for the administration of physical and logical access controls.

2-5

A.

An effective enterprise risk management (ERM) framework is

not a key success factor for an information security program.

B.

Commitment from senior management provides the basis to

achieve success in implementing an information security

program.

C.

Although an effective information security budgeting process will contribute to success, senior management commitment is the key

element.

D.

Program planning is important but will not be sufficient without senior management commitment.

2-6

A.

Evaluating the activities of boards and committees providing oversight is an important aspect of governance and should be measured.

B.

Providing strategic IT drivers is irrelevant to the evaluation of IT governance performance measures.

C.

Adhering to regulatory reporting standards and definitions is irrelevant to the evaluation of IT governance performance measures.

D.

Evaluating the IT department is irrelevant to the evaluation of IT governance performance measures.

2-7

A.

The roles of security administration and change management are

incompatible functions. The level of security administration

access rights could allow changes to go undetected.

B.

Computer operations and system development is the incorrect

choice because this would make it possible for an operator to run a program that he/she had amended.

C.

The combination of system development and change control

would allow program modifications to bypass change control

approvals.

D.

It is common for system development and maintenance to be

undertaken by the same person. In both, the programmer

requires access to the source code in the development

environment but should not be allowed access in the

production environment.

2-8

A.

Approval of database administration (DBA) activities does not

prevent the combination of conflicting functions. Review of

access logs and activities is a detective control.

B.

Segregation of duties (SoD) will prevent combination of

conflicting functions. This is a preventive control, and it is the most critical control over DBA.

C.

If DBA activities are improperly approved, review of access logs and activities may not reduce the risk.

D.

Reviewing the use of database tools does not reduce the risk

because this is only a detective control and does not prevent

combination of conflicting functions.

2-9

A.

Origination, in conjunction with recording and correction, does

not enable the transaction to be authorized for processing and

committed within the system of record.

B.

Authorization should be separated from all aspects of record

keeping (origination, recording and correction). Such a

separation enhances the ability to detect the recording of

unauthorized transactions.

C.

Recording, in conjunction with origination and correction, does not enable the transaction to be authorized for processing and committed within the system of record.

D.

Correction, in conjunction with origination and recording, does not enable the transaction to be authorized for processing and committed within the system of record.

2-10 A.

Logging changes to development libraries would not detect changes to production libraries.

B.

In smaller organizations, it generally is not appropriate to recruit additional staff to achieve a strict segregation of duties (SoD).

The IS auditor must look at alternatives.

C.

The IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed by a third party on a regular basis. This would be a compensating control process.

D.

Access controls to prevent the operator from making program

modifications require a third party to do the changes, which may not be practical in a small organization.

PART A: IT GOVERNANCE

2.0 INTRODUCTION

IT governance is not an isolated discipline. Rather, it is an integral part of a comprehensive enterprise/corporate governance program and shares the objectives of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that resources are used responsibly. The IT governance process usually starts with setting objectives for an enterprise's IT, and then a continuous loop is created to measure performance, benchmark against objectives, and move forward or change direction, as appropriate.

2.1 IT GOVERNANCE AND IT STRATEGY

Ethical issues, decision-making and overall practices within an organization must be fostered through corporate governance practices. These make up the system by which enterprises are directed and controlled. The board of directors is responsible for the governance of the enterprise. IT governance consists of the leadership and organizational structures and processes that ensure the enterprise sustains and extends strategies and objectives.

Corporate governance involves a set of relationships among a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. The purpose of corporate governance is to help build an environment of trust, transparency and accountability necessary for fostering long-term investment, financial stability and business integrity, thereby supporting stronger growth and more inclusive societies (OECD, *G20/OECD Principles of Corporate Governance*, OECD Publishing, Paris, 2015).

A corporate governance framework is being increasingly used by government

bodies globally in an effort to reduce the frequency and impact of inaccurate financial reporting and provide greater transparency and accountability.

Many of these government regulations include a requirement that senior management sign off on the adequacy of internal controls and include an assessment of organizational internal controls in the organization's financial reports. **Figure 2.1** illustrates the components of an enterprise governance framework.

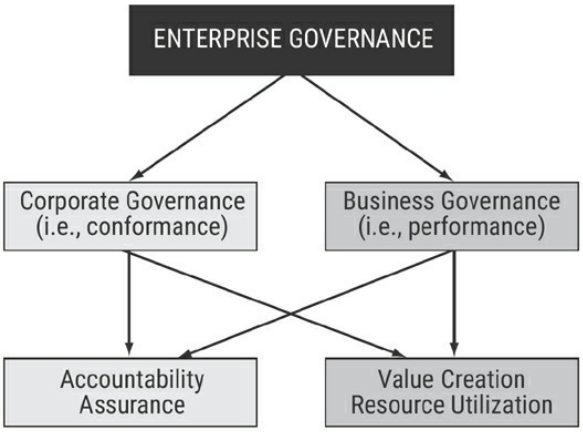
2.1.1 ENTERPRISE GOVERNANCE OF INFORMATION AND TECHNOLOGY

Enterprise governance of information and technology (EGIT) implies a system in which all stakeholders, including the board, senior management, internal customers and departments such as finance, provide input into the IT

decision-making process. EGIT is the responsibility of the board of directors and executive management. In other words, EGIT is about the stewardship of IT resources on behalf of all stakeholders (internal and external) who expect their interests to be met. The board of directors responsible for this stewardship will look to management to implement the necessary systems and IT controls.

The purpose of EGIT is to direct IT endeavors to ensure that IT aligns with and supports the enterprise's objectives and its realization of promised benefits. Additionally, IT should enable the enterprise by exploiting opportunities and maximizing benefits. IT resources should be used responsibly, and IT-related risk should be managed appropriately.

Figure 2.1—The Enterprise Governance Framework



Source: International Federation of Accountants, *Enterpreise Governance: Getting the Balance Right*, USA, 2003, *www.ifac.org*

Implementing an EGIT framework addresses these issues by implementing practices that provide feedback on value delivery and risk management. The broad processes are:

• **IT resource management**—Focuses on maintaining an updated inventory of all IT resources and addresses the risk management process

• **Performance measurement**—Focuses on ensuring that all IT resources perform as expected to deliver value to the business and identify risk early on. This process is based on performance indicators that are optimized for value delivery and from which any deviation might lead to risk.

• **Compliance management**—Focuses on implementing processes that address legal and regulatory policy and contractual compliance

requirements

ISACA's COBIT framework, which was developed to help enterprises optimize the value of information assets, makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes. COBIT's view on this key distinction between governance and management is:

• **Governance**—Ensures that stakeholder needs, conditions and options are

evaluated to determine balanced, agreed-on enterprise objectives; direction is set through prioritization and decision-making; and performance and compliance are monitored against agreed-on direction and objectives

• **Management**—Plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives

EGIT, one of the domains of enterprise governance, comprises the body of issues addressed in considering how IT is applied within the enterprise.

Effective enterprise governance focuses both individual and group expertise and experience in specific areas where it can be most effective. For a long time, IT was considered only an enabler of an organization strategy; now IT

is seen as an integral part of the strategy. Senior management agrees that strategic alignment between IT and enterprise objectives has become a critical success factor (CSF) for organizations and cannot be seen simply as either IT management or IT specialist operations. Rather, IT has to receive guidance and supervision from senior management and oversight by the board of directors. The key element of EGIT is the alignment of business and IT that leads to the achievement of business value.

Fundamentally, EGIT is concerned with two issues: (1) that IT delivers value to the business and (2) that IT risk is managed. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise.

2.1.2 GOOD PRACTICES FOR EGIT

The purpose of an IT governance system is to satisfy stakeholder needs and generate value from the use of IT. This value is a balance among benefits, risk and resources.

EGIT has become significant due to a number of factors:

• Business managers and boards demanding a better return from IT

investments (i.e., that IT deliver what the business needs to enhance stakeholder value)

• Concern over the generally increasing level of IT expenditure

• The need to meet regulatory requirements for IT controls in areas such as privacy and financial reporting (e.g., the US Sarbanes-Oxley Act, Basel Accords, the European Union (EU) General Data Protection Regulation

[GDPR]) and in specific sectors such as finance, pharmaceuticals and healthcare

• The selection of service providers and the management of service outsourcing and acquisition (e.g., cloud computing)

• IT governance initiatives that include adoption of control frameworks and good practices to help monitor and improve critical IT activities to increase business value and reduce business risk (e.g., emerging risk related to cybersecurity)

• The need to optimize costs by following, where possible, standardized rather than specially developed approaches

• The growing maturity and consequent acceptance of well-regarded frameworks

• The need for enterprises to assess how they are performing against generally accepted standards and their peers (i.e., benchmarking) The processes to evaluate, direct and monitor are integrated end to end into the governance process and focus on evaluation, direction and monitoring of the following:

• Conformance and performance

• The system of internal controls

• Compliance with external requirements

2.1.3 AUDIT'S ROLE IN EGIT

Enterprises are governed by generally accepted good practices, ensured by the establishment of controls. Good practices guide organizations in determining how to use resources. Results are measured and reported, providing input to the cyclical revision and maintenance of controls.

Similarly, IT is governed by good practices, which ensure that the organization's information and related technology support the enterprise's business objectives

(i.e., strategic alignment), deliver value, use resources responsibly, manage risk appropriately and measure performance.

Audit plays a significant role in the successful implementation of EGIT

within an organization. Audit is well positioned to provide leading practice recommendations to senior management to help improve the quality and

effectiveness of the IT governance initiatives implemented.

As an entity that monitors compliance, audit helps ensure compliance with EGIT initiatives implemented within an organization. The continual monitoring, analysis and evaluation of metrics associated with EGIT

initiatives require an independent and balanced view to ensure a qualitative assessment that subsequently facilitates the qualitative improvement of IT

processes and associated EGIT initiatives.

Reporting on EGIT involves auditing at the highest level in the organization and may cross divisional, functional or departmental boundaries. The IS

auditor should confirm that the terms of reference state the:

• Scope of the work, including a clear definition of the functional areas and issues to be covered.

• Reporting line to be used, where EGIT issues are identified to the highest level of the organization.

• IS auditor’s right of access to information both within the organization and from third-party service providers.

The organizational status and skill sets of the IS auditor should be considered for appropriateness with regard to the nature of the planned audit. When this is found to be insufficient, the hiring of an independent third party to manage or perform the audit should be considered by an appropriate level of management.

In accordance with the defined role of the IS auditor, the following aspects related to EGIT need to be assessed:

• How enterprise governance and EGIT are aligned

• Alignment of the IT function with the organization's mission, vision, values, objectives and strategies

• Achievement of performance objectives (e.g., effectiveness and efficiency) established by the business and the IT function

• Legal, environmental, information quality, fiduciary, security and privacy requirements

• The control environment of the organization

• The inherent risk within the IS environment

• IT investment/expenditure

2.1.4 INFORMATION SECURITY GOVERNANCE

The strategic direction of a business is defined by business goals and objectives. Information security must support business activities to be of value to the organization. Information security governance is a subset of corporate governance that provides strategic direction for security activities and ensures that objectives are achieved. It ensures that information security risk is appropriately managed and enterprise information resources are used responsibly. According to the US National Institute of Standards and Technology (NIST) Special Publication 800-100, *Information Security Handbook: A Guide for Managers*:

Information security governance can be defined as the process of establishing and maintaining a framework and supporting

management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

To achieve effective information security governance, management must establish and maintain a framework to guide the development and

management of a comprehensive information security program that supports business objectives.

An information security governance framework generally consists of the following elements:

• A comprehensive security strategy intrinsically linked with business objectives

• Governing security policies that address each aspect of strategy, controls and regulation

• A complete set of standards for each policy to ensure that procedures and guidelines comply with policy

• An effective security organizational structure void of conflicts of interest

• Institutionalized monitoring processes to ensure compliance and provide

feedback on effectiveness

This framework provides the basis for the development of a cost-effective information security program that supports the organization’s business goals.

The objective of the information security program is a set of activities that provides assurance that information assets are given a level of protection commensurate with their value or the risk their compromise poses to the organization.

Effective Information Security Governance

Because of its prominent role within IT governance processes, information security governance has risen to one of the highest levels of focused activity with specific value drivers: confidentiality, integrity and availability of information; continuity of services; and protection of information assets.

Security has become a significant governance issue as a result of global networking, rapid technological innovation and change, increased dependence on IT, increased sophistication of threat agents and exploits, and an extension of the enterprise beyond its traditional boundaries. Therefore, information security is an important and integral part of IT governance.

Negligence in this regard will diminish an organization’s capacity to mitigate risk and take advantage of IT opportunities for business process improvement.

Boards of directors and chief executive officers (CEOs) globally are accountable and responsible for information security governance. The CEO is accountable to the board of directors for information security governance and responsible for its discharge through the executive management and the organization and resources under his/her charge.

The members of senior management who approve security policies should come from varied operations and staff functions within the enterprise to ensure that there is a fair representation of the enterprise as a whole. This is to minimize any potential leaning toward a specific business priority or technology overhead or security concerns. Typically, the board-level committee approving security policies may include directors, the CEO, the chief operating officer (COO), the chief financial officer (CFO), the chief risk

officer (CRO), the chief information officer (CIO), the chief technology officer (CTO), the head of human resources (HR), the chief of audit, the chief compliance officer (CCO) and legal. Policy approval should be, to the greatest extent possible, based on consensus.

Information is a key resource for all enterprises, and from the time that information is created or received to the moment that it is destroyed, technology plays a significant role. IT is increasingly advanced and has become pervasive in enterprises and in social, public and business environments. As a result, enterprises and their executives strive to accomplish the following:

- Maintain high-quality information to support business decisions

- Generate business value from IT-enabled investments (i.e., achieve strategic goals and realize business benefits through effective and innovative use of IT)

- Achieve operational excellence through the reliable and efficient application of technology

- Maintain IT-related risk at an acceptable level

- Optimize the cost of IT services and technology

• Comply with ever-increasing relevant laws, regulations, contractual agreements and policies

Until recently, protection efforts have focused on the information systems that collect, process and store information rather than the information itself.

This approach has become too narrow to accomplish the overall security that is necessary. Information security takes the broader view that data, as well as the information and knowledge based on them, must be adequately protected regardless of where they are created, received, processed, transported or stored, and disposed. This applies particularly to situations in which data are shared easily over the Internet through blogs, newsfeeds, peer-to-peer or social networks, or websites. Thus, the reach of protection efforts should encompass not only the process that generates the information, but also the continued preservation of information generated as a result of the controlled processes.

Some of the major trends that global business is experiencing today include

the outsourcing of in-house processes and increased use of cloud computing.

Information security coverage extends beyond the geographic boundary of the enterprise's premises in onshoring and offshoring models being adopted by organizations.

The basic outcomes of effective information security governance include strategic alignment, risk management, compliance and value delivery. These outcomes are enabled through the development of:

• **Performance measurement**—Measurement, monitoring and reporting on information security processes to ensure that specific, measurable, attainable, realistic and timely (SMART) objectives are achieved. The following should be accomplished to achieve performance measurement:

– A defined, agreed-on and meaningful set of metrics properly aligned with strategic objectives

– A measurement process that will help identify shortcomings and provide feedback on progress made in resolving issues

– Independent assurance provided by external assessments and audits

• **Resource management**—Use of information security knowledge and

infrastructure efficiently and effectively. To achieve resource management, the following should be considered:

– Ensure that knowledge is captured and available.

– Document security processes and practices.

– Develop security architecture(s) to define and use infrastructure resources efficiently.

• **Process integration**—A focus on the integration of an organization's management assurance processes for security. Security activities are at times fragmented and segmented in silos with different reporting structures. This makes it difficult, if not impossible, to seamlessly integrate them. Process integration serves to improve overall security and operational efficiencies.

2.1.5 INFORMATION SYSTEMS STRATEGY

Information systems are crucial in the support, sustainability and growth of enterprises. Previously, governing boards and senior management executives could minimize their involvement in the direction and development of IS

strategy, leaving most decisions to functional management. However, this approach is no longer acceptable or possible with increased or total dependency on IS for day-to-day operations and successful growth. Along with the near-complete dependence on IS for functional and operational activities, organizations also face numerous internal and external threats ranging from IS resource abuse to cybercrime, fraud, and errors and omissions. IS strategic processes are integral components within the organization's governance structure to provide reasonable assurance that both existing and emerging business goals and objectives will be attained as critical facilitators for enhancement of competitive advantage.

2.1.6 STRATEGIC PLANNING

Strategic planning from an IS standpoint relates to the long-term direction an enterprise wants to take in leveraging IT for improving its business processes.

Under the responsibility of top management, factors to consider include identifying cost-effective IT solutions in addressing problems and opportunities

that confront the enterprise and developing action plans for identifying and acquiring needed resources. In developing strategic plans, generally three to five years in duration, enterprises should ensure that the plans are fully aligned and consistent with the overall organizational goals and objectives. IT department management, along with the IT steering committee and the strategy committee (which provides valuable strategic input related to stakeholder value), play a key role in the development and implementation of the plans.

Effective IS strategic planning involves a consideration of the enterprise's requirements for new and revised information systems and the IT

organization's capacity to deliver new functionality through well-governed projects. Determining requirements for new and revised information systems involves a systematic consideration of the enterprise's strategic intentions, how these translate into specific objectives and business initiatives, and what IT capabilities will be needed to support these objectives and initiatives.

In assessing IT capabilities, the existing system's portfolio should be reviewed in terms of functional fit, cost and risk. Assessing IT's capacity to deliver involves a review of an organization's technical IT infrastructure and

key support processes (e.g., project management, software development and maintenance practices, security administration, and help desk services) to determine whether expansion or improvement is necessary. It is important for the strategic planning process to encompass the delivery of new systems and technology and consider return on investment (ROI) on existing IT and the decommissioning of legacy systems. The strategic IT plan should balance the cost of maintenance of existing systems against the cost of new initiatives or systems to support business strategies.

IS auditors should pay full attention to the importance of IS strategic planning, taking management control practices into consideration. IT

strategic plans should be synchronized with the overall business strategy. IS

auditors must focus on the importance of a strategic planning process or planning framework. Particular attention should be paid to the need to assess how operational, tactical or business development plans from the business are considered in IT strategy formulation, contents of strategic plans, requirements for updating and communicating plans, and monitoring and evaluation

requirements. IS auditors also should consider how the CIO or senior IT management is involved in the creation of the overall business strategy. A lack of involvement of IT in the creation of the business strategy indicates that there is a risk that the IT strategy and plans will not be aligned with the business strategy.

2.1.7 BUSINESS INTELLIGENCE

Business intelligence (BI) is a broad field of IT that encompasses the collection and analysis of information to assist decision-making and assess organizational performance.

Investments in BI technology can be applied to enhance understanding of a wide range of business questions. Some typical areas in which BI is applied for measurement and analysis purposes include the following:

• Process cost, efficiency and quality

• Customer satisfaction with product and service offerings

• Customer profitability, including determination of which attributes are useful predictors of customer profitability

• Staff and business unit achievement of key performance indicators

• Risk management (e.g., by identifying unusual transaction patterns and accumulation of incident and loss statistics)

The interest in BI as a distinct field of IT activity is due to a number of factors:

• **The increasing size and complexity of modern organizations**—The result is that even fundamental business questions cannot be properly answered without establishing serious BI capability.

• **Pursuit of competitive advantage**—Most organizations have, for many years, automated their basic, high-volume activities. Significant organizationwide IT investment, such as enterprise resource planning (ERP) systems, is now common place. Many companies have or are now investing in Internet technology as a means of distributing

products/services and for supply chain integration. However, utilization of IT to

maintain and extend a business's knowledge capital represents a new opportunity to use technology to gain an advantage over competitors.

• **Legal requirements**—Legislation exists to enforce the need for companies to understand the "whole of business." Financial institutions must now be able to report on all accounts/instruments their customers have and all transactions against those accounts/instruments, including any suspicious transaction patterns.

To deliver effective BI, organizations need to design and implement (progressively, in most cases) a data architecture. A complete data architecture consists of two components:

• The enterprise data flow architecture (EDFA)

• A logical data architecture

An example of optimized EDFA is depicted in **figure 2.2**. Explanations of the various layers/components of this data flow architecture follow:

• **Presentation/desktop access layer**—This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suites, and purpose-built applications such as balanced scorecards (BSCs) and digital dashboards. Power users will have the ability to build their own queries and reports while other users will interact with the data in predefined ways.

• **Data source layer**—Enterprise information derives from a number of sources: operational data, external data and nonoperational data.

• **Core data warehouse**—A core data warehouse (DW) is where all (or at least the majority of) the data of interest to an organization are captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. While there is not unanimous agreement, many pundits suggest the DW should hold fully normalized data to support the flexibility to deal with complex and changing business structures.

• **Data mart layer**—Data marts represent subsets of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data marts may be relational databases or some form of online

analytical processing (OLAP) data structure (also known as a data cube). Data marts have a simplified structure compared to the normalized DW.

• **Data staging and quality layer**—This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data get loaded to the core DW.

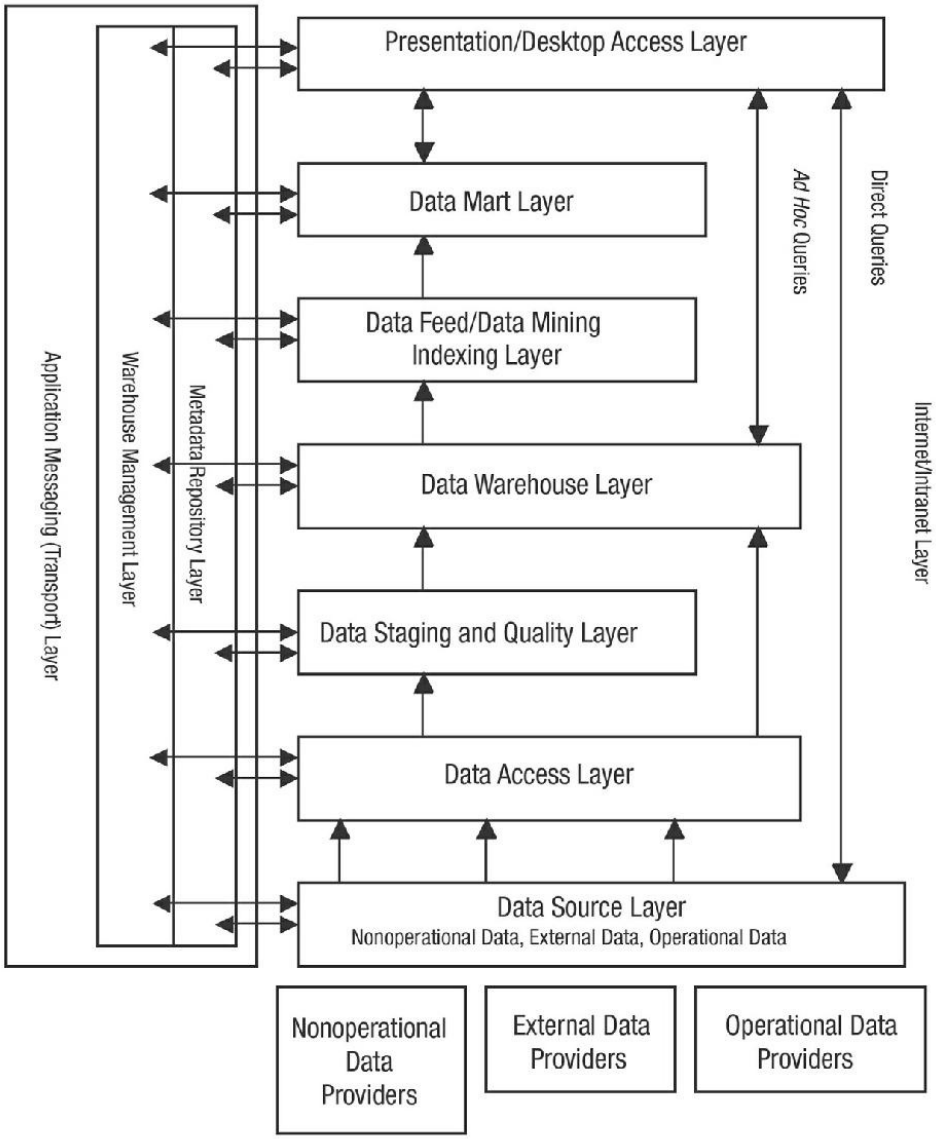
This layer needs to be able to deal with problems periodically thrown up by operational systems such as changes to account number formats and reuse of old account and customer numbers (when the DW still holds information on the original entity).

• **Data access layer**—This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know exactly how these data stores are organized.

• **Data preparation layer**—This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to precalculate the values that are loaded into OLAP data repositories to increase access speed. Specialist data mining also normally requires preparation of data. Data mining explores large volumes of data to determine patterns and trends of information.

• **Metadata repository layer**—Metadata are data about data. The information held in the metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules. Ideally, information in the metadata

Figure 2.2—Data Flow Architecture Sample



layer can be directly sourced by software operating in the other layers, as required.

• **Warehouse management layer**—The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in the administration of security.

• **Application messaging layer**—This layer is concerned with transporting information between the various layers. In addition to business data, this

layer encompasses generation, storage and targeted communication of control

messages.

• **Internet/intranet layer**—This layer is concerned with basic data communication. Included here are browser-based user interfaces and Transmission Control Protocol/Internet Protocol (TCP/IP) networking.

The construction of the logical data architecture for an organization is a major undertaking that would normally be undertaken in stages. One reason for separating logical data model determination by business domain is that different parts of large business organizations often deal with different transaction sets, customers and products.

Ultimately, the data architecture needs to be structured to accommodate the needs of the organization in the most efficient manner. Factors to consider include the types of transactions in which the organization engages, the entities that participate in or form part of these transactions (e.g., customers, products, staff and communication channels), and the dimensions

(hierarchies) that are important to the business (e.g., product and organization hierarchies).

With modern DWs, storage capacity is not really an issue. Therefore, the goal should be to obtain the most granular or atomic data possible. The lowest-level data are most likely to have attributes that can be used for analysis purposes that would be lost if summarized data are loaded.

Various analysis models used by data architects/analysts include the following:

• **Context diagrams**—Outline the major processes of an organization and the external parties with which the business interacts

• **Activity or swim-lane diagrams**—Deconstruct business processes

• **Entity relationship diagrams**—Depict data entities and how they relate.

These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operatives be involved in the process. This way, proper understanding can be obtained of the business purpose and context of the

data. This also mitigates the risk of the replication of suboptimal data configurations from existing systems and databases into the DW.

Data Governance

To maximize the value an organization obtains from its BI initiatives, an effective data governance process needs to be in place.

An important part of the governance process involves determining which BI initiatives to fund, what priority to assign to initiatives and how to measure their ROI. This is particularly important because the investment needed to build BI infrastructure, such as a DW, is considerable. Additionally, the scope and complexity of an organizationwide DW means that, realistically, it must be built in stages.

A recommended practice in the area of BI funding governance is to establish a business/IT advisory team that allows different functional perspectives to be represented, recommends investment priorities and establishes cross-organizational benefit measures. Final funding decisions should rest with a technology steering committee that is comprised of senior management. A further important part of overall BI governance is data governance. Aspects to be considered here include establishing standard definitions for data, business rules and metrics; identifying approved data sources; and establishing standards for data reconciliation and balancing.

2.2 IT-RELATED FRAMEWORKS

Organizations can either fail or succeed based on how they approach and use technology. To address this, EGIT frameworks have been developed to help enterprise leaders protect the integrity of their enterprise's information assets and deliver value to stakeholders. The frameworks help organizations address business issues through governance and management of information and technology, starting with aligning high-level strategic objectives with operational-level objectives and then direct work outcomes. The key to maximizing value is to consider EGIT synergistically in the overall enterprise governance hierarchy.

Examples of EGIT frameworks include the following:

• **COBIT** was developed by ISACA to support EGIT by providing a framework

to ensure that IT is aligned with the business, IT enables the business and maximizes benefits, IT resources are used responsibly, and IT

risk is managed appropriately. COBIT provides tools to assess and measure the performance of IT processes within an organization.

• The **International Organization for Standardization**

(ISO)/International Electrotechnical Commission (IEC) 27000 series is a set of best practices that provides guidance to organizations

implementing and maintaining information security programs. ISO/IEC

27001 has become a well-known standard in the industry.

• The **Information Technology Infrastructure Library (ITIL®**) was developed by the UK Office of Government Commerce (OGC), in

partnership with the IT Service Management Forum, and is a detailed framework with hands-on information regarding how to achieve successful operational service management of IT. It also includes business value delivery.

• **The Open Information Security Management Maturity Model (O-**

ISM3) is a process-based ISM maturity model for security.

• ***ISO/IEC 38500:2015: Information technology—Governance of IT for***

the organization provides guiding principles for members of governing bodies of organizations on the effective, efficient and acceptable use of IT

within an organization.

• **ISO/IEC 20000** is a specification for service management that is aligned with ITIL's service management framework. It is divided into two parts.

ISO/IEC 20000-1:2018 consists of specific requirements for service management improvement, and ISO/IEC 20000-2:2012 provides guidance and examples for the application of ISO/IEC 20000-1:2018.

• ***ISO 3100:2018: Risk management—Guidelines*** provides guidelines on and a

common approach to risk management for organizations.

2.3 IT STANDARDS, POLICIES AND PROCEDURES

There is broad range of interpretation of policies, standards, procedures and guidelines. The definitions used in this document agree with the major standards bodies and should be adopted to preclude miscommunication.

Policies and standards are considered tools of governance and management, respectively, and procedures and guidelines the purview of operations.

2.3.1 STANDARDS

A standard is a mandatory requirement, code of practice or specification approved by a recognized external standards organization. **Professional** standards refer to standards issued by professional organizations, such as ISACA, with related guidelines and techniques that assist the professional in implementing and complying with other standards. Strong standards are necessary in current fast-moving environments. They help ensure

effectiveness and reliability of products and services and are necessary to the trust and effectiveness needed to ensure continued growth. They are updated as needed to ensure they address the latest thinking and technology.

2.3.2 POLICIES

Policies are the high-level statements of management intent, expectations and direction. Well-developed high-level policies in a mature organization can remain fairly static for extended periods. An example of an effective high-level policy statement on access control could be: *Information resources shall be controlled in a manner that effectively precludes unauthorized access*. Policies can be considered the “constitution” of governance and must be clearly aligned with and support the strategic objectives of the organization.

In addition to corporate policies that set the tone for the organization as a whole, individual divisions and departments should define lower-level policies. The lower-level policies should be consistent with the corporate-level policies. These apply to the employees and operations of these units and focus at the operational level.

Management should review all policies periodically. Ideally, these documents should specify a review date, which the IS auditor should check for currency.

Policies need to be updated to reflect new technology, changes in environment (e.g., regulatory compliance requirements), and significant changes in business processes in exploiting IT for efficiency and

effectiveness in productivity or competitive gains. Policies formulated must support achievement of business objectives and implementation of IS

controls. The broad policies at a higher level and the detailed policies at a lower level need to be in alignment with the business objectives.

IS auditors should understand that policies are a part of the audit scope and test the policies for compliance. IS controls should flow from the enterprise's policies, and IS auditors should use policies as a benchmark for evaluating compliance. However, if policies exist that hinder the achievement of business objectives, these policies must be identified and reported for improvement. The IS auditor should also consider the extent to which the policies apply to third parties or outsourcers, the extent to which third parties or outsourcers comply with the policies, and whether the policies of the third parties or outsourcers are in conflict with the enterprise's policies.

Information Security Policy

An information security policy is a set of rules and/or statements developed by an organization to protect its information and related technology. A security policy for information and related technology helps guide behaviors and is a first step toward building the security infrastructure for technology-driven organizations. Policies will often set the stage in terms of what tools and procedures are needed for the organization. Information security policies must balance the level of control with the level of productivity. Also, the cost of a control should never exceed the expected benefit to be derived. In designing and implementing these policies, the organizational culture will play an important role. The information security policy must be approved by senior management and should be documented and communicated, as

appropriate, to all employees, service providers and business partners (e.g., suppliers). The information security policy should be used by IS auditors as a reference framework for performing various IS audit assignments. The adequacy

and appropriateness of the security policy could also be an area of review for the IS auditor.

The information security policy should state management's commitment and set out the organization's approach to managing information security. The ISO/IEC 27001 standard (or equivalent standards) as well as the 27002

guideline may be considered a benchmark for the content covered by the information security policy document.

The policy document should contain the following elements:

• A definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing

• A statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives

• A framework for setting control objectives and controls, including the structure of risk assessment and risk management

• A brief explanation of the information security policies, principles, standards and compliance requirements of particular importance to the organization including:

– Compliance with legislative, regulatory and contractual requirements

– Information security education, training and awareness requirements

– Business continuity management

– Consequences of information security policy violations

• A definition of general and specific responsibilities for information security management, including reporting information security incidents

• References to documentation that may support the policy (e.g., more detailed security policies, standards, and procedures for specific information systems, or security rules with which users should comply) The information security policy should be communicated throughout the organization to users in a form that is

accessible and understandable to the intended reader. The information security policy might be a part of a general policy document and may be suitable for distribution to third parties and outsourcers of the organization as long as care is taken not to disclose sensitive organizational information. All employees or third parties having access to information assets should be required to sign off on their understanding and willingness to comply with the information security policy at the time they are hired and on a regular basis thereafter (e.g., annually) to account for policy changes over time.

Depending upon the need and appropriateness, organizations may document

information security policies as a set of policies. Generally, the following policy concerns are addressed:

• A **high-level information security policy** should include statements on confidentiality, integrity and availability.

• A **data classification policy** should describe the classifications, levels of control at each classification and responsibilities of all potential users including ownership.

• An **acceptable use policy** is a comprehensive policy that includes information for all information resources (hardware, software, networks, Internet, etc.) and describes the organizational permissions for the usage of IT and information-related resources.

• An **end-user computing policy** describes the parameters and usage of desktop, mobile computing and other tools by users.

• **Access control policies** describe the method for defining and granting access to users to various IT resources.

Review of the Information Security Policy

The information security policy should be reviewed at planned intervals (at least annually) or when significant changes to the enterprise, its business operations or inherent security-related risk occur to ensure its continuing suitability, adequacy and effectiveness. The information security policy should have an owner who has approved management responsibility for the development, review and evaluation of the policy. The review should include assessing opportunities for

improvement to the organization’s information security policy and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

The maintenance of the information security policy should consider the results of these reviews. There should be defined management review procedures, including a schedule or period for the review.

The input to the management review should include:

• Feedback from interested parties

• Results of independent reviews

• Status of preventive, detective and corrective actions

• Results of previous management reviews

• Process performance and information security policy compliance

• Changes that could affect the organization’s approach to managing information security, including changes to the organizational environment; business circumstances; resource availability; contractual, regulatory and legal conditions; or technical environment

• Use of outsourcers or offshore of IT or business functions

• Trends related to threats and vulnerabilities

• Reported information security incidents

• Recommendations provided by relevant authorities

The output from management review should include any decisions and actions related to:

• Improvement in the alignment of information security with business objectives.

• Improvement of the organization’s approach to managing information security and its processes.

• Improvement of control objectives and controls.

• Improvement in the allocation of resources and/or responsibilities.

A record of management reviews should be maintained and management approval for the revised policy should be obtained.

Note: This review is performed by management to address the changes in environmental factors.

While reviewing the policies, the IS auditor needs to assess the following:

• Basis on which the policy has been defined—generally based on a risk management process

• Appropriateness of these policies

• Contents of policies

• Exceptions to the policies, clearly noting in which area the policies do not apply and why (e.g., password policies may not be compatible with legacy applications)

• Policy approval process

• Policy implementation process

• Effectiveness of implementation of policies

• Awareness and training

• Periodic review and update process

2.3.3 PROCEDURES

Procedures are documented, defined steps for achieving policy objectives.

They must be derived from the parent policy and must implement the spirit (intent) of the policy statement. Procedures must be written in a clear and concise manner, so they may be easily and properly understood by those governed by them. Procedures document business and aligned IT processes

(administrative and operational) and the embedded controls. Procedures are formulated by process owners as an effective translation of policies.

Generally, procedures are more dynamic than their respective parent policies.

Procedures must reflect the regular changes in business and aligned IT focus and environment. Therefore, frequent reviews and updates of procedures are essential if they are to be relevant. IS auditors review procedures to identify/evaluate and, thereafter, test controls over business and aligned IT

processes. The controls embedded in procedures are evaluated to ensure that they fulfill necessary control objectives while making the process as efficient and practical as possible. Where operational practices do not match documented procedures or where documented procedures do not exist, it is difficult (for management and auditors) to identify controls and ensure they are in continuous operation.

One of the most critical aspects related to procedures is that they should be well known by the people they govern. A procedure that is not thoroughly known by the personnel who are to use it is, essentially, ineffective.

Therefore, attention should be paid to deployment methods and automation of mechanisms to store, distribute and manage IT procedures.

Quite often, procedures are embedded in information systems, which is an advisable practice to further integrate these procedures within the enterprise.

2.3.4 GUIDELINES

Guidelines for executing procedures are also the responsibility of operations.

Guidelines should contain information that will be helpful in executing the procedures. This can include clarification of policies and standards, dependencies, suggestions and examples, narrative clarifying the procedures, background information that may be useful, and tools that can be used.

Guidelines can be useful in many other circumstances as well, but they are considered here in the context of information security governance.

2.4 ORGANIZATIONAL STRUCTURE

Organizational structure is a key component to governance. It identifies the key decision-making entities in an enterprise. The following section provides guidance for organizational structures, roles and responsibilities within EGIT.

Actual structures may differ depending on the size, industry and location of an enterprise.

2.4.1 IT GOVERNING COMMITTEES

Traditionally, organizations have had executive-level steering committees to handle IT issues that are relevant organizationwide. There should be a clear understanding of both the IT strategy and steering levels. ISACA has issued a document offering a clear analysis (**figure 2.3**). Organizations may also have other executive-and mid-management-led committees guiding IT operations, such as an IT executive committee, IT governance committee, IT investment committee and/or IT management committee.

Note: The analysis of IT steering committee responsibilities is information the CISA should know.

2.4.2 ROLES AND RESPONSIBILITIES OF SENIOR

MANAGEMENT AND BOARDS OF DIRECTORS

Information security governance requires strategic direction and impetus. It requires commitment, resources and assignment of responsibility for information security management as well as a means for the board to determine that its intent has been met.

Effective information security governance can be accomplished only by involvement of the board of directors and/or senior management in approving policy; ensuring appropriate monitoring; and reviewing metrics, reports and trend analysis.

Board of Directors

Members of the board need to be aware of the organization’s information assets and their criticality to ongoing business operations. This can be accomplished by periodically providing the board with the high-level results of comprehensive risk assessments and business impact analysis (BIA). It may also be

accomplished by business dependency assessments of

information resources. These activities should include approval by board members of the assessment of key assets to be protected, which helps ensure that protection levels and priorities are appropriate to a standard of due care.

The tone at the top must be conducive to effective security governance. It is unreasonable to expect lower-level personnel to abide by security measures if they are not exercised by senior management. Senior management

endorsement of intrinsic security requirements provides the basis for ensuring that security expectations are met at all levels of the enterprise. Penalties for noncompliance must be defined, communicated and enforced from the board level down.

Figure 2.3—Analysis of IT Steering Committee Responsibilities Level

IT Strategy Committee

IT Steering Committee

Responsibility

• Provides insight and advice to the

• Decides the overall level of IT

board on topics such as:

spending and how costs will be

– The relevance of developments in

allocated

IT from a business perspective

• Aligns and approves the enterprise’s

– The alignment of IT with the

IT architecture

business direction

• Approves project plans and budgets,

– The achievement of strategic IT

setting priorities and milestones

objectives

• Acquires and assigns appropriate

– The availability of suitable IT

resources

resources, skills and

• Ensures that projects continuously

infrastructure to meet the

meet business requirements,

strategic objectives

including reevaluation of the

– Optimization of IT costs,

business case

including the role and value

• Monitors project plans for delivery

delivery of external IT sourcing

of expected value and desired

– Risk, return and competitive

outcomes, on time and within

aspects of IT investments

budget

– Progress on major IT projects

• Monitors resource and priority

– The contribution of IT to the

conflict between enterprise divisions

business (i.e., delivering the

and the IT function as well as

promised business value)

between projects

– Exposure to IT risk, including

• Makes recommendations and

compliance risk

requests for changes to strategic

– Containment of IT risk

plans (priorities, funding,

– Direction to management relative

technology approaches, resources,

to IT strategy

etc.)

– Drivers and catalysts for the

• Communicates strategic goals to

board’s IT strategy

project teams

• Is a major contributor to

management’s IT governance

responsibilities and practices

Authority

• Advises the board and management

• Assists the executive in the delivery

on IT strategy

of the IT strategy

• Is delegated by the board to provide

• Oversees day-to-day management of

input to the strategy and prepare its

IT service delivery and IT projects

approval

• Focuses on implementation

• Focuses on current and future

strategic IT issues

Membership

• Board members and specialists who

• Sponsoring executive

are not board members

• Business executives (key users)

• Chief information officer (CIO)

• Key advisors as required (i.e., IT,

audit, legal, finance)

The board of directors is the accountable and liable body for the organization.

Accountability means the board takes the responsibility of ensuring the organization follows the laws, behaves in an ethical manner, and makes effective use of its resources.

Senior Management

Implementing effective security governance and defining the strategic security objectives of an organization is a complex task. As with any other major initiative, it must have leadership and ongoing support from executive management to succeed. Developing an effective information security strategy requires integration with and cooperation of business process owners. A successful outcome is the alignment of information security activities in support of business objectives. The extent to which this is

achieved will determine the cost-effectiveness of the information security program in achieving the desired objective of providing a predictable, defined level of assurance for business information and processes and an acceptable level of impact from adverse events.

Information Security Standards Committee

Security affects all aspects of an organization to some extent, and it must be

pervasive throughout the enterprise to be effective. To ensure that all stakeholders impacted by security considerations are involved, many organizations use a steering committee comprised of senior representatives of affected groups. This facilitates achieving consensus on priorities and trade-offs. It also serves as an effective communications channel and provides an ongoing basis for ensuring the alignment of the security program with business objectives. It can also be instrumental in achieving modification of behavior toward a culture more conducive to good security.

The chief information security officer (CISO) will primarily drive the information security program to have realistic policies, standards, procedures and processes that are implementable and auditable and to achieve a balance of performance in relation to security. However, it is necessary to involve the affected groups in a deliberating committee, which may be called the information security standards committee (ISSC). The ISSC includes members from C-level executive management and senior managers from IT, application owners, business process owners, operations, HR, audit and legal.

The committee will deliberate on the suitability of recommended controls and good practices in the context of the organization, including the secure configuration of operating systems (OSs) and databases. The auditor's presence is required to make the systems auditable by providing for suitable audit trails and logs. Legal is required to advise on liability and conflicts with the law. This is not a prescriptive list of members to be included on the ISSC.

Members of the committee may be modified to suit the context of the organizations, and other members may be co-opted as necessary to suit the control objectives in question.

Chief Information Security Officer

All organizations have a CISO whether or not anyone holds the exact title.

The responsibilities may be performed by the CIO, CTO, CFO or, in some cases, the CEO, even when there is an information security office or director in place. The scope and breadth of information security is such that the authority required and the responsibility taken will inevitably make it a senior officer or top management responsibility. This could include a position such as a CRO or a CCO. Legal responsibility will, by default, extend up the command structure and

ultimately reside with senior management and the board of directors. Failure to recognize this and implement appropriate governance structures can result in senior management being unaware of this responsibility and the related liability. It also usually results in a lack of effective alignment of business objectives and security activities.

Increasingly, prudent management is elevating the position of information security officer to a senior management position, as organizations increasingly recognize their dependence on information and the growing threats to it.

IT Steering Committee

The enterprise's senior management should appoint a planning or steering committee to oversee the IT function and its activities. A high-level steering committee for information systems is an important factor in ensuring that the IT department is in harmony with the corporate mission and objectives.

Although not a common practice, it is highly desirable that a member of the board of directors who understands the risk and issues is responsible for IT

and is chair of this committee. The committee should include representatives from senior management, each line of business, corporate departments, such as HR and finance, and the IT department.

The committee's duties and responsibilities should be defined in a formal charter. Members of the committee should know IT department policies, procedures and practices. They should have the authority to make decisions within the group for their respective areas.

This committee typically serves as a general review board for major IS

projects and should not become involved in routine operations. Primary functions performed by this committee include:

• Reviewing the long- and short-range plans of the IT department to ensure

that they align with the corporate objectives.

• Reviewing and approving major acquisitions of hardware and software within the limits approved by the board of directors.

• Approving and monitoring major projects and the status of IS plans and budgets, establishing priorities, approving standards and procedures, and monitoring overall IS performance.

• Reviewing and approving sourcing strategies for select or all IS activities, including insourcing or outsourcing, and the globalization or offshoring of functions.

• Reviewing adequacy of resources and allocation of resources in terms of time, personnel and equipment.

• Making decisions regarding centralization versus decentralization and assignment of responsibility.

• Supporting development and implementation of an enterprisewide information security management program.

• Reporting to the board of directors on IS activities.

Note: Responsibilities will vary from enterprise to enterprise; the responsibilities listed are the most common responsibilities of the IT steering committee. Each enterprise should have formally documented and approved terms of reference for its steering committee, and IS auditors should familiarize themselves with the IT steering committee documentation and understand the major responsibilities that are assigned to its members. Many enterprises may refer to this committee with a different name. The IS auditor needs to identify the group that performs the previously mentioned functions.

Matrix of Outcomes and Responsibilities

The relationships between the outcomes of effective security governance and management responsibilities are shown in **figure 2.4**. This matrix is not meant to be comprehensive but is intended merely to indicate some primary tasks and the management level responsible for those tasks. Depending on the nature of the organization, the titles may vary, but the roles and responsibilities should exist even if different labels are used.

Note: While **figure 2.4** is not specifically tested in the CISA exam, the CISA candidate should be aware of this information.

Figure 2.4—Relationships of Security Governance Outcomes to Management Responsibilities

Management Level	Strategic Alignment	Risk Management	Value Delivery	Performance Measurement	Resource Management	ProcessAssurance
Board of directors	Require demonstrable alignment.	• Establish risk tolerance. • Oversee a policy of risk management. • Ensure regulatory compliance.	Require reporting of security activity costs.	Require reporting of security effectiveness.	Oversee a policy of knowledge management and resource utilization.	Oversee a policy of assurance process integration.
Executive management	Institute processes to integrate security with business objectives.	• Ensure that roles and responsibilities include risk management in all activities. • Monitor regulatory compliance.	Require business case studies of security activities.	Require monitoring and metrics for security initiatives.	Ensure processes for knowledge capture and efficiency metrics.	Provide oversight of all assurance functions and plans for integration.
Steering committee	• Review and assist security strategy and integrationefforts. • Ensure that business owners support integration.	Identify emerging risk, promote business unit security practices and identify compliance issues.	Review and advise on the adequacy of security initiatives to serve business functions.	Review and advise whether security initiatives meet business objectives.	Review processes for knowledge capture and dissemination.	• Identify critical business processes and assurance providers. • Direct assurance integration efforts.
CISO/ information security management	Develop the security strategy, oversee the security program and initiatives, and liaise with business process owners for ongoing alignment.	• Ensure that risk and business impact assessments are conducted. • Develop risk mitigation strategies. • Enforce policy and regulatory compliance.	Monitor utilization and effectiveness of security resources.	Develop and implement monitoring and metrics approaches, and direct and monitor security activities.	Develop methods for knowledge capture and dissemination, and develop metrics for effectiveness and efficiency.	• Liaise with other assurance providers. • Ensure that gaps and overlaps are identified and addressed.
Audit executives	Evaluate and report on degree of alignment.	Evaluate and report on corporate risk management practices and results.	Evaluate and report on efficiency.	Evaluate and report on degree of effectiveness of measures in place and metrics in use.	Evaluate and report on efficiency or resource management.	Evaluate and report on effectiveness of assurance processes performed by different areas of management.

Source: ISACA, *Information Security Governance: Guidance for Information Security Managers*, 2008

2.4.3 IT ORGANIZATIONAL STRUCTURE AND RESPONSIBILITIES

An IT department can be structured in different ways. One such format is shown in **figure 2.5**. The organizational chart depicted includes functions related to security, applications development and maintenance, technical support for network and systems administration, and operations. The organizational structure shows the IT department typically headed by an IT

manager/director or, in large organizations, by a CIO.

Note: The CISA exam does not test specific job responsibilities because they may vary among organizations. However, universally known

responsibilities such as business owners, information security functions and executive management might be tested, especially when access controls and data ownership are tested. A CISA should be familiar with SoD.

-
-
-

IT Roles and Responsibilities

An organizational chart is an important item for all employees to know, because it provides a clear definition of the department's hierarchy and authorities. Additionally, job descriptions; responsible, accountable, consulted, informed (RACI) charts; and swimlane workflow diagrams provide IT department employees a more complete and clear direction regarding their (and others') roles and responsibilities. The IS auditor should spend time in an auditee's area to observe and determine whether the formal job description and structures coincide with real ones and are adequate.

Generally, the following IT functions should be reviewed:

• **Systems development manager**—Systems development managers are responsible for programmers and analysts who implement new systems and maintain existing systems.

• **Project management**—Project managers are responsible for planning and executing IS projects and may report to a project management office or to the development organization. Project management staff use budgets assigned to them for the delivery of IS initiatives and report on project progress to the IT steering committee. Project managers play a central role in executing the vision of the IT strategy and IT steering committees by planning, coordinating and delivering IT projects to the enterprise.

• **Help desk (service desk)**—More and more companies find a help desk function critical for their IT departments. A help desk is a unit within an

organization that responds to technical questions and problems faced by users. Most software companies have help desks. Questions and answers can be delivered by telephone, fax, email or instant messaging. Help desk personnel may use third-party help desk software that enables them to quickly find answers to common questions. A procedure to record the problems reported, solved and escalated should be in place for analysis of the problems/questions. It helps in monitoring the user groups and improving the software/information processing facility (IPF) services.

– Help desk/support administration includes the following activities: Acquire hardware/software (HW/SW) on behalf of end users.

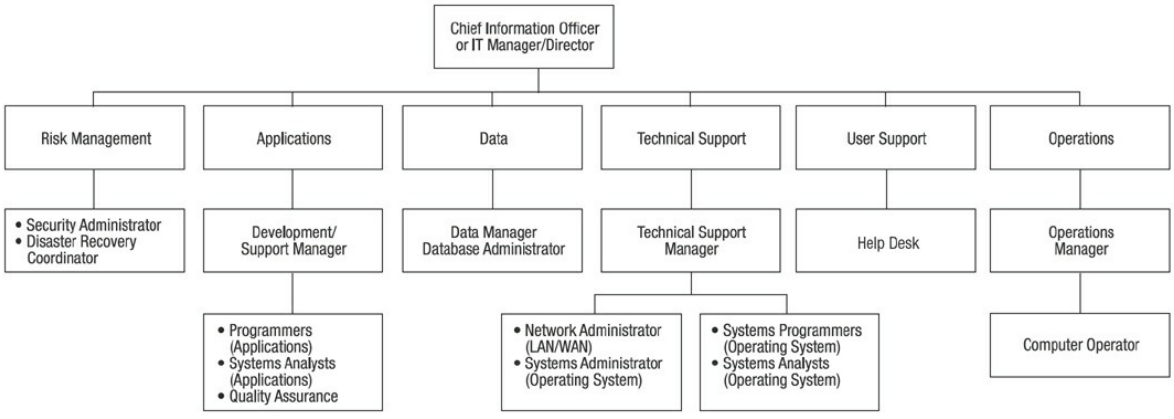
Assist end users with HW/SW difficulties.

Train end users to use HW/SW and databases; answer end-user

queries.

-
-
-

Figure 2.5—IT Department Organization



Monitor technical developments and inform end users of pertinent developments.

Determine the source of problems with production systems and initiate corrective actions. Inform end users of problems with HW/SW or

databases that could affect their control of the installation of HW/SW

upgrades.

Initiate changes to improve efficiency.

• **End user**—End users are responsible for operations related to business application services. There is a small distinction between the terms “end user” and “user.” End user is slightly more specific and refers to someone who will access a business application. User is broader and could refer to administrative accounts and accounts to access platforms.

• **End-user support manager**—The end-user support manager acts as a liaison between the IT department and the end users.

• **Data management**—Data management personnel are responsible for the data architecture in larger IT environments and tasked with managing data as corporate assets.

• **Quality assurance (QA) manager**—The QA manager is responsible for negotiating and facilitating quality activities in all areas of IT.

• **Information security management**—This is a function that generally needs to be separate from the IT department and headed by a CISO. The CISO may report to the CIO or have a dotted-line (indirect reporting) relationship to the CIO. Even when the security officer reports to the CIO,

there is a possibility of conflict because the goals of the CIO are to efficiently provide continuous IT services whereas the CISO may be less interested in cost reduction if this impacts the quality of protection.

Vendor and Outsourcer Management

With the increase in outsourcing, including the use of multiple vendors, dedicated staff may be required to manage the vendors and outsourcers. This may necessitate staff performing the following functions:

• Acting as the prime contact for the vendor and outsourcer within the IT

function

• Providing direction to the outsourcer on issues and escalating internally within the organization and IT function

• Monitoring and reporting on the service levels to management

• Reviewing changes to the contract due to new requirements and obtaining IT approvals

Infrastructure Operations and Maintenance

An **operations manager** is responsible for computer operations personnel, including all the staff required to run the data center efficiently and effectively (e.g., computer operators, librarians, schedulers and data control personnel). The data center includes the servers and mainframe, peripherals such as high-speed printers, networking equipment, magnetic media, and storage area networks. It constitutes a major asset investment and impacts the organization's ability to function effectively.

The **control group** is responsible for the collection, conversion and control of input, and the balancing and distribution of output to the user community.

The supervisor of the control group usually reports to the IPF operations manager. The input/output control group should be in a separate area where only authorized personnel are permitted since they handle sensitive data.

Media Management

Media management is required to record, issue, receive and safeguard all program and data files that are maintained on removable media. Depending on the size of the organization, this function may be assigned to a full-time individual or a member of operations who also performs other duties.

This is a crucial function. Therefore, many organizations provide additional support through the use of software that assists in maintaining inventory, movement, version control and configuration management.

Data Entry

Data entry is critical to the information processing activity and includes batch entry or online entry. In most organizations personnel in user departments do

their own data entry online. In many online environments, data are captured from the original source (e.g., electronic data interchange

[EDI] input documents, data captured from bar codes for time management, departmental store inventory). The user department and the system application must have controls in place to ensure that data are validated, accurate, complete and authorized.

Supervisory Control and Data Acquisition

With the advancement of technology and need to acquire data at their origination site, automated systems for data acquisition are being deployed by organizations. These systems include barcode readers or systems that are referred to as **supervisory control and data acquisition** (SCADA). The term SCADA usually refers to centralized systems that monitor and control entire sites, or complexes of systems spread out over large areas (on the scale of kilometers or miles). These systems are typical of industrial plants, steel mills, power plants, electrical facilities and similar. Most site control is performed automatically by remote terminal units (RTUs) or by

programmable logic controllers (PLCs). Host control functions are usually restricted to basic site overriding or supervisory level intervention. An example of automated systems for data acquisition are those used on oil rigs to measure and control the extraction of oil and to control the temperature and flow of water. Data acquisition begins at the RTU or PLC level and includes meter readings and equipment status reports that are communicated to SCADA as required. Data are then compiled and formatted in such a way that a control room operator using human machine interfacing (HMI) networks can make supervisory decisions to adjust or override normal RTU

or PLC controls. Data may also be fed to a history log, often built on a commodity database management system, to allow trending and other analytical auditing.

SCADA applications traditionally used dedicated communication lines, but there has been a significant migration to the Internet. This has obvious advantages, among them easier integration in the company business applications. However, a disadvantage is that many such companies are nation-critical infrastructures and become easy prey to cyberattacks.

Systems Administration

The **systems administrator** is responsible for maintaining major multiuser computer systems, including local area networks (LANs), wireless local area networks (WLANs), wide area networks (WANs), virtual

machine/server/network environments, personal area networks (PANs), storage area networks (SANs), intranets and extranets, and mid-range and mainframe systems. Typical duties include the following activities:

- Adding and configuring new workstations and peripherals
- Setting up user accounts
- Installing systemwide software
- Performing procedures to prevent/detect/correct the spread of viruses
- Allocating mass storage space

Small organizations may have one systems administrator, whereas larger enterprises may have a team of them. Some mainframe-centric organizations may refer to a systems administrator as a systems programmer.

Security Administration

Security administration begins with management's commitment.

Management must understand and evaluate security risk and develop and enforce a written policy that clearly states the standards and procedures to be followed. The duties of the **security administrator** should be defined in the policy. To provide adequate SoD, this individual should be a full-time employee who may report directly to the infrastructure director. However, in a small organization, it may not be practical to hire a full-time individual for this position. The individual performing the function should ensure that the various users are complying with the corporate security policy and controls are adequate to prevent unauthorized access to the company assets (including data, programs and equipment). The security administrator's functions usually include:

- Maintaining access rules to data and other IT resources.

• Maintaining security and confidentiality over the issuance and maintenance of authorized user IDs and passwords.

• Monitoring security violations and taking corrective action to ensure that adequate security is provided.

• Periodically reviewing and evaluating the security policy and suggesting necessary changes to management.

• Preparing and monitoring the security awareness program for all employees.

• Testing the security architecture to evaluate the security strengths and detect possible threats.

• Working with compliance, risk management and audit functions to ensure that security is appropriately designed and updated based on audit feedback or testing.

Database Administration

The **database administrator** (DBA), as custodian of an organization's data, defines and maintains the data structures in the corporate database system.

The DBA must understand the organization and user data and data

relationship (structure) requirements. This position is responsible for the security of the shared data stored on database systems. The DBA is responsible for the actual design, definition and proper maintenance of the corporate databases. The DBA usually reports directly to the director of the IPF. The DBA's role includes:

• Specifying the physical (computer-oriented) data definition.

• Changing the physical data definition to improve performance.

• Selecting and implementing database optimization tools.

• Testing and evaluating programming and optimization tools.

• Answering programmer queries and educating programmers in the database structures.

• Implementing database definition controls, access controls, update controls and concurrency controls.

• Monitoring database usage, collecting performance statistics and tuning the database.

• Defining and initiating backup and recovery procedures.

The DBA has the tools to establish controls over the database and the ability to override these controls. The DBA also has the capability of gaining access to all data, including production data. It is usually not practical to prohibit or completely prevent access to production data by the DBA. Therefore, the IT

department must exercise close control over database administration through the following approaches:

• SoD

• Management approval of DBA activities

• Supervisor review of access logs and activities

• Detective controls over the use of database tools

Systems Analyst

Systems analysts are specialists who design systems based on the needs of the user and are usually involved during the initial phase of the system development life cycle (SDLC). These individuals interpret the needs of the user and develop requirements and functional specifications as well as high-level design documents. These documents enable programmers to create a specific application.

Security Architect

Security architects evaluate security technologies; design security aspects of the network topology, access control, identity management and other security systems; and establish security policies and security requirements. One may argue that systems analysts perform the same role; however, the set of skills required is quite different. The deliverables (e.g., program specifications versus

policies, requirements, architecture diagrams) are different as well.

Security architects should also work with compliance, risk management and audit functions to incorporate their requirements and recommendations for security into the security policies and architecture.

System Security Engineer

The **system security engineer**, as defined under *ISO/IEC 21827:2008: Information technology—Security techniques—Systems Security Engineering*

—Capability Maturity Model, provides technical information system security engineering support to the organization that encompasses the following:

• Project life cycles, including development, operation, maintenance and

decommissioning activities

• Entire organizations, including management, organizational and engineering activities

• Concurrent interactions with other disciplines, such as system software and hardware, human factors, test engineering, system management, operation and maintenance

• Interactions with other organizations, including acquisition, system management, certification, accreditation and evaluation

Applications Development and Maintenance

Applications staff are responsible for developing and maintaining applications. Development can include developing new code or changing the existing setup or configuration of the application. Staff develop the programs or change the application setup that will ultimately run in a production environment. Therefore, management must ensure that staff cannot modify production programs or application data. Staff should work in a test-only environment and turn their work to another group to move programs and application changes into the production environment.

Infrastructure Development and Maintenance

Infrastructure staff are responsible for maintaining the systems software, including the OS. This function may require staff to have broad access to the entire system. IT management must closely monitor activities by requiring that electronic logs capture this activity and are not susceptible to alteration.

Infrastructure staff should have access to only the system libraries of the specific software they maintain. Usage of domain administration and superuser accounts should be tightly controlled and monitored.

Network Management

Today many organizations have widely dispersed IPFs. They may have a central IPF, but they also make extensive use of:

• LANs at branches and remote locations

• WANs, where LANs may be interconnected for ease of access by authorized personnel from other locations

• Wireless networks established through mobile devices

Network administrators are responsible for key components of this infrastructure (e.g., routers, switches, firewalls, network segmentation, performance management, remote access). Because of geographical

dispersion, each LAN may need an administrator. Depending on the policy of the company, these administrators can report to the director of the IPF or, in a decentralized operation, may report to the end-user manager, although at least a dotted line to the director of the IPF is advisable. This position is responsible for technical and administrative control over the LAN. This includes ensuring that transmission links are functioning correctly, backups of the system are occurring, and software/hardware purchases are authorized and installed properly. In smaller installations this person may be responsible for security administration over the LAN. The LAN administrator should have no application programming responsibilities but may have systems programming and end-user responsibilities.

2.4.4 SEGREGATION OF DUTIES WITHIN IT

Actual job titles and organizational structures vary greatly from one organization

to another depending on the size and nature of the business.

However, an IS auditor should obtain enough information to understand and document the relationships among the various job functions, responsibilities and authorities, and assess the adequacy of the SoD. SoD avoids the possibility that a single person could be responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner and in the normal course of business processes. SoD is an important means by which fraudulent and/or malicious acts can be discouraged and prevented. Duties that should be segregated include:

• Custody of the assets

• Authorization

• Recording transactions

If adequate SoD does not exist, the following could occur:

• Misappropriation of assets

• Misstated financial statements

• Inaccurate financial documentation (i.e., errors or irregularities)

• Undetected improper use of funds or modification of data

• Undetected unauthorized or erroneous changes or modification of data and programs

When duties are segregated, access to the computer, production data library, production programs, programming documentation, and OS and associated utilities can be limited, and potential damage from the actions of any one person is, therefore, reduced. The IS and end-user departments should be organized to achieve adequate SoD. See **figure 2.6** for a guideline of the job responsibilities that should not be combined.

Note: The SoD control matrix (**figure 2.6**) is not an industry standard but a guideline indicating which positions should be separated and which require compensating controls when combined. The matrix illustrates potential SoD

issues and should not be viewed or used as an absolute; rather, it should be used to help identify potential conflicts so that proper questions may be asked to identify compensating controls.

In actual practice, functions and designations may vary in different enterprises. Further, depending on the nature of the business processes and technology deployed, risk may vary. However, it is important for an IS

auditor to understand the functions of each of the designations specified in this manual. IS auditors need to understand the risk of combining functions, as indicated in **figure 2.6**. In addition, depending on the complexity of the applications and systems deployed, an automated tool may be required to evaluate the actual access a user has against a SoD matrix. Most tools come with a predefined SoD matrix that must be tailored to an organization's IT

and business processes, including any additional functions or risk areas that are not included in the delivered SoD matrix.

Regarding privileged users of the system, remote logging (sending system logs to a separate log server) should be enabled, so that the privileged users do not have access to their own logs. For example, the activities of the DBA may be remotely logged to another server where an official in the IT

department can review/audit the DBA's actions. The activities of system

administrators may be similarly monitored via separation of log review duties on an independent log server.

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness when duties cannot be appropriately segregated. The organization structure and roles should be considered when determining the appropriate controls for the relevant environment. For example, an organization may not have all the positions described in the matrix or one person may be responsible for many of the roles described. The size of the IT department may also be an important factor that should be considered (i.e., certain combinations of roles in an IT

department of a certain size should never be used). However, if for some reason combined roles are required, then compensating controls should be developed and put in place.

Segregation-of-duties Controls

Several control mechanisms can be used to strengthen SoD. The controls are described in the following sections.

Transaction Authorization

Transaction authorization is the responsibility of the user department.

Authorization is delegated to the degree that it relates to the particular level of responsibility of the authorized individual in the department. Periodic checks must be performed by management and audit to detect the

unauthorized entry of transactions.

Figure 2.6—Segregation of Duties Control Matrix

	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database	Network	Systems	Security Administrator	SystemsProgrammer	Quality Assurance
Control Group		X	X	X		X	X	X	X	X		X	
Systems Analyst	X			X	X		X				X		X
Application Programmer	X			X	X	X	X	X	X	X	X	X	X
Help Desk and Support Manager	X	X	X		X	X		X	X	X		X	
End User		X	X	X			X	X	X			X	X
Data Entry	X		X	X			X	X	X	X	X	X	
Computer Operator	X	X	X		X	X		X	X	X	X	X	
Database Administrator	X		X	X	X	X	X		X	X		X	
Network Administrator	X		X	X	X	X	X	X					
System Administrator	X		X	X		X	X	X				X	
Security Administrator		X	X			X	X					X	
Systems Programmer	X		X	X	X	X	X	X		X	X		X
Quality Assurance		X	X		X							X	

X—Combination of these functions may create a potential control weakness.

Custody of Assets

Custody of corporate assets must be determined and assigned appropriately.

The data owner usually is assigned to a particular user department, and that individual's duties should be specific and in writing. The owner of the data has responsibility for determining authorization levels required to provide adequate security, while the administration group is often responsible for implementing and enforcing the security system.

Access to Data

Controls over access to data are provided by a combination of physical, system and application security in the user area and the IPF. The physical environment must be secured to prevent unauthorized personnel from accessing the various tangible devices connected to the central processing

unit, thereby permitting access to data. System and application security are additional layers that may prevent unauthorized individuals from gaining access to corporate data. Access to data from external connections continues to be a growing concern because of the Internet. Therefore, IT management has added responsibilities to protect information assets from unauthorized access.

Access control decisions are based on organizational policy and two generally accepted standards of practice—SoD and least privilege. Controls for effective use must not disrupt the usual workflow more than necessary or place too much burden on auditors or authorized users. Further access must be conditional and access controls must adequately protect all of the organization's resources.

Policies establish levels of sensitivity—such as top secret, secret, confidential and unclassified—for data and other resources. These levels should be used for guidance on the proper procedures for handling information resources.

The levels may be also used as a basis for access control decisions.

Individuals are granted access to only those resources at or below a specific level of sensitivity. Labels are used to indicate the sensitivity level of electronically stored documents. Policy-based controls may be characterized as either mandatory or discretionary.

Authorization Forms

System owners must provide IT with formal authorization forms (either hard copy or electronic) that define the access rights of each individual. In other words, managers must define who should have access to what. Authorization forms must be evidenced properly with management-level approval.

Generally, all users should be authorized with specific system access via a formal request from management. In large companies or in those with remote sites, signature authorization logs should be maintained, and formal requests should be compared to the signature log. Access privileges should be reviewed periodically to ensure they are current and appropriate to the user's job functions.

User Authorization Tables

The IT department should use the data from the authorization forms to build and maintain user authorization tables. These define who is authorized to update, modify, delete and/or view data. These privileges are provided at the system, transaction or field level. In effect, these are user access control lists.

These authorization tables must be secured against unauthorized access by additional password protection or data encryption. A control log should record all user activity and appropriate management should review this log.

All exception items should be investigated.

Compensating Controls for Lack of Segregation of Duties

In a small business where the IT department may consist of only four to five people, compensating control measures must exist to mitigate the risk resulting from a lack of SoD. Before relying on system-generated reports or functions as compensating controls, the IS auditor should carefully evaluate the reports, applications and related processes for appropriate controls, including testing and access controls to make changes to the reports or functions. Compensating controls include the following:

• **Audit trails** are an essential component of all well-designed systems. Audit trails help the IT and user departments as well as the IS auditor by providing a map to retrace the flow of a transaction. Audit trails enable the user and IS

auditor to recreate the actual transaction flow from the point of origination to its existence on an updated file. In the absence of adequate SoD, good audit trails may be an acceptable compensating control. The IS

auditor should be able to determine who initiated the transaction, the time of day and date of entry, the type of entry, what fields of information it contained, and what files it updated.

• **Reconciliation** is ultimately the responsibility of the user department. In some organizations, limited reconciliation of applications may be performed by the data control group with the use of control totals and balance sheets. This type of independent verification increases the level of confidence that the application processed successfully and the data are in proper balance.

• **Exception reporting** should be handled at the supervisory level and should require evidence, such as initials on a report, noting that the exception has been handled properly. Management should also ensure that exceptions are resolved in a timely manner.

• **Transaction logs** may be manual or automated. An example of a manual log is a record of transactions (grouped or batched) before they are submitted for processing. An automated transaction log provides a record of all transactions processed and is maintained by the computer system.

• **Supervisory reviews** may be performed through observation and inquiry or remotely.

• **Independent reviews** are carried out to compensate for mistakes or intentional failures in following prescribed procedures. These reviews are particularly important when duties in a small organization cannot be appropriately segregated. Such reviews will help detect errors or irregularities.

2.4.5 AUDITING IT GOVERNANCE STRUCTURE AND IMPLEMENTATION

While many conditions concern the IS auditor when auditing the IT function, some of the more significant indicators of potential problems include:

• Excessive costs

- Budget overruns
- Late projects
- High staff turnover
- Inexperienced staff
- Frequent HW/SW errors
- An excessive backlog of user requests
- Slow computer response time
- Numerous aborted or suspended development projects
- Unsupported or unauthorized HW/SW purchases
- Frequent HW/SW upgrades
- Extensive exception reports
- Exception reports that were not followed up
- Lack of succession plans
- A reliance on one or two key personnel
- Lack of adequate training

Reviewing Documentation

IS auditors should review the following governance documents:

- IT strategies, plans and budgets
- Security policy documentation
- Organization/functional charts
- Job descriptions

• IT steering committee reports

• System development and program change procedures

• Operations procedures

• HR manuals

• QA procedures

The documents should be assessed to determine whether:

• They were created as management authorized and intended.

• They are current and up to date.

2.5 ENTERPRISE ARCHITECTURE

An area of IT governance that is receiving increasing attention is enterprise architecture (EA). Essentially, EA involves documenting an organization's IT

assets in a structured manner to facilitate understanding, management and planning for IT investments. An EA often involves both a current state and an optimized future-state representation (e.g., a road map).

The current focus on EA is a response to the increasing complexity of IT, the complexity of modern organizations, and an enhanced focus on aligning IT

with business strategy and ensuring that IT investments deliver real returns.

The Framework for Enterprise Architecture: Background, Description and Utility, a groundbreaking work in the field of EA, was first published by John Zachman in the late 1980s. The Zachman framework continues to be a starting point for many contemporary EA projects. Zachman reasoned that constructing IT systems had considerable similarities to building construction. In both cases there is a range of participants who become involved at differing stages of the project. In building construction, one moves from the abstract to the physical using models and representations (such as blueprints, floor plans and wiring diagrams). Similarly with IT, different artifacts (such as diagrams, flowcharts, data/class models and code)

are used to convey different aspects of an organization's systems at progressively greater levels of detail.

The basic Zachman framework is shown in **figure 2.7.**

The ultimate objective is to complete all cells of the matrix. At the outset of an EA project, most organizations will have difficulty providing details for every cell, particularly at the highest level.

In attempting to complete an EA, organizations can address the challenge either from a technology perspective or a business process perspective.

Technology-driven EA attempts to clarify the complex technology choices faced by modern organizations. The idea is to provide guidance on issues such as whether and when to use advanced technical environments (e.g., JavaEE or .NET) for application development, how to better connect intra-and interorganizational systems, how to "web-enable" legacy and ERP

applications (without extensive rewrite), whether to insource or outsource IT

functions, and whether and when to use solutions such as virtualization and cloud computing.

Business-process-driven EA attempts to understand an organization in terms of its core value-adding and -supporting processes. The idea is that by understanding processes, their constituent parts and the technology that supports them, business improvement can be obtained as aspects are progressively redesigned and replaced. The genesis for this type of thinking can be traced back to the work of Harvard University professor Michael Porter, and particularly his business value chain model. The effort to model business processes is being given extra impetus by a number of industrywide business models such as the telecommunications industry's enhanced Telecom Operations Map (eTOM) and the Supply Chain Operations

Reference (SCOR) model. The contents from a business process model can be mapped to upper tiers of the Zachman framework. After the mapping is completed, an organization can consider the optimal mix of technologies needed to support its business processes.

When auditing infrastructure and operations, the IS auditor should follow the

Figure 2.7—Zachman Framework for Enterprise Architecture						
	Data	Functional (Application)	Network (Technology)	People (Organization)	Process (Workflow)	Strategy
Scope						
Enterprise model						
Systems model						
Technology model						
Detailed representation						

overall EA and use the EA as a main source of information. Further, the IS

auditor should ensure that the systems are in line with the EA and meet the organization's objectives.

2.6 ENTERPRISE RISK MANAGEMENT

Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what countermeasures (safeguards or controls), if any, to take in reducing risk to an acceptable level (i.e., residual risk), based on the value of the information resource to the organization.

Effective risk management begins with a clear understanding of the organization's appetite for risk. This drives all risk management efforts and, in an IT context, impacts future investments in technology, the extent to which IT assets are protected and the level of assurance required. Risk management encompasses identifying, analyzing, evaluating, treating, monitoring and communicating the impact of risk on IT processes. Having defined risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Depending on the type of risk and its significance to the business, management and the board may choose to:

• **Avoid**—Eliminate the risk by eliminating the cause (e.g., where feasible, choose not to implement certain activities or processes that would incur risk).

• **Mitigate**—Lessen the probability or impact of the risk by defining, implementing and monitoring appropriate controls.

• **Share/Transfer**—Share risk with partners or transfer via insurance coverage, contractual agreement or other means.

• **Accept**—Formally acknowledge the existence of the risk and monitor it.

Therefore, risk can be avoided, reduced, transferred or accepted. An organization can also choose to reject risk by ignoring it, which can be dangerous and should be considered a red flag by the IS auditor.

2.6.1 DEVELOPING A RISK MANAGEMENT PROGRAM

Steps to developing a risk management program include:

• **Establish the purpose of the risk management program**—The first step is to determine the organization's purpose for creating a risk management program. The program's purpose may be to reduce the cost of insurance or reduce the number of program-related injuries. By determining its intention before initiating risk management planning, the organization can define KPIs and evaluate the results to determine the program's effectiveness.

Typically, senior management, with the board of directors, sets the tone and goals for the risk management program.

• **Assign responsibility for the risk management plan**—The second step is to designate an individual or team responsible for developing and implementing the organization's risk management program. While the team is primarily responsible for the risk management plan, a successful program requires the integration of risk management within all levels of the organization. Operations staff and board members should assist the risk management committee in identifying risk and developing suitable loss control and intervention strategies.

2.6.2 RISK MANAGEMENT PROCESS

To ensure that an enterprise manages its risk consistently and appropriately, an organization should identify and establish a repeatable process to manage its IT risk. Basic steps in the risk management process are described in the following sections.

Step 1: Asset Identification

The first step in the process is the identification and collection of relevant data to enable effective IT-related risk identification, analysis and reporting.

This will help to identify information resources or assets that need protection

because they are vulnerable to threats. In this context, a threat is any circumstance or event with the potential to cause harm (such as destruction, disclosure, modification of data and/or denial of service) to an information resource. The purpose of the classification may be either to prioritize further investigation and identify appropriate protection (simple classification based on asset value) or to enable a standard model of protection to be applied (classification in terms of criticality and sensitivity). Examples of typical assets associated with information and IT include:

• Information and data

• Hardware

• Software

• Documents

• Personnel

Other, more traditional business assets for consideration are buildings, stock of goods (inventory), and cash and intangible assets such as goodwill or image/reputation.

Step 2: Evaluation of Threats and Vulnerabilities to Assets

The second step in the process is to assess threats and vulnerabilities associated with the information resource and the likelihood of their occurrence. Common classes of threats are:

• Errors

• Malicious damage/attack

• Fraud

• Theft

• Equipment/software failure

IT risk occurs because of threats (or predisposing conditions) that have the potential to exploit vulnerabilities associated with use of information resources. Vulnerabilities are characteristics of information resources that can be exploited by a threat to cause harm. Examples of vulnerabilities are:

• Lack of user knowledge

• Lack of security functionality

• Inadequate user awareness/education (e.g., poor choice of passwords)

• Untested technology

• Transmission of unprotected communications For a vulnerability to be realized, there must be either a human or environmental threat to exploit the vulnerability. Typical human threat actors (or threats caused by humans) are:

• Novices (kiddie scripters)

• Hacktivists

• Criminal

• Terrorists

• Nation-states

• Riots and civil unrest

Typical environmental threats include the following:

• Floods

• Lightning

• Tornados

• Hurricanes

• Earthquakes

Step 3: Evaluation of the Impact

The result of a threat agent exploiting a vulnerability is called an impact. The impact can vary in magnitude, affected by severity and duration. In commercial organizations, threats usually result in a direct financial loss in the short term or an ultimate (indirect) financial loss in the long term.

Examples of such losses include:

• Direct loss of money (cash or credit)

• Breach of legislation (e.g., unauthorized disclosure)

• Loss of reputation/goodwill

• Endangering of staff or customers

• Breach of confidence

• Loss of business opportunity

• Reduction in operational efficiency/performance

• Interruption of business activity

Step 4: Calculation of Risk

After the elements of risk have been established, they are combined to form

an overall view of risk. A common method of combining the elements is to calculate the following for each threat: probability of occurrence × magnitude of impact. This will give a measure of overall risk.

The risk is proportional to the estimated likelihood of the threat and the value of the loss/damage.

Step 5: Evaluation of and Response to Risk

After risk has been identified, existing controls can be evaluated or new controls designed to reduce the vulnerabilities to an acceptable level. These controls are referred to as countermeasures or safeguards and include actions, devices,

procedures or techniques (i.e., people, processes or products). The strength of a control can be measured in terms of its inherent or design strength and the likelihood of its effectiveness. Characteristics of controls that should be considered when evaluating control strength include whether the controls are preventive, detective or corrective, manual or automated, and formal (i.e., documented in procedure manuals and evidence of their operation is maintained) or *ad hoc*.

Residual risk, the remaining level of risk after controls have been applied, can be further reduced by identifying those areas in which more control is required. An acceptable level of risk target can be established by management (risk appetite). Risk in excess of this level should be reduced by the implementation of more stringent controls. Risk below this level should be evaluated to determine whether an excessive level of control is being applied and whether cost savings can be made by removing these excessive controls.

Final acceptance of residual risk considers:

- Organizational policy
- Risk appetite
- Risk identification and measurement
- Uncertainty incorporated in the risk assessment approach
- Cost and effectiveness of implementation
- Cost of control versus benefit

It is important to realize that IT risk management needs to operate at multiple levels, including:

- **The operational level**—At the operational level, one is concerned with risk that could compromise the effectiveness and efficiency of IT systems and supporting infrastructure, the ability to bypass system controls, the possibility of loss or unavailability of key resources (e.g., systems, data, communications, personnel, premises), and failure to comply with laws and regulations.
- **The project level**—Risk management needs to focus on the ability to

understand and manage project complexity and, if this is not done effectively, to handle the consequent risk that the project objectives will not be met.

• **The strategic level**—The risk focus shifts to considerations such as how well the IT capability is aligned with the business strategy, how it compares with that of competitors and the threats (as well as the opportunities) posed by technological change.

The identification, evaluation and management of IT risk at various levels are the responsibility of different individuals and groups within the organization.

However, these individuals and groups should not operate separately because risk at one level or in one area may also impact risk in another. A major system malfunction could impair an organization's ability to deliver customer service or deal with suppliers, and it could have strategic implications that require top management attention. Similarly, problems with a major project could have strategic implications. Also, as projects deliver new IT systems and infrastructure, the new operational risk environment needs to be considered.

In summary, the risk management process should achieve a cost-effective balance between the application of security controls as countermeasures and the significant threats. Some of the threats are related to security issues that can be extremely sensitive for some industries.

2.6.3 RISK ANALYSIS METHODS

The most common risk analysis methods include qualitative, semiquantitative and quantitative. Each has advantages and limitations.

Qualitative Analysis Methods

Qualitative risk analysis methods use word or descriptive rankings to describe the impacts or likelihood. They are the simplest and most frequently used methods—used mostly where the risk level is low. They are normally based on checklists and subjective risk ratings such as high, medium or low.

While often less complicated and less time-consuming than the other methods, they also lack the rigor that is customary for accounting and management.

Semiquantitative Analysis Methods

In semiquantitative analysis, the descriptive rankings are associated with a numeric scale. Such methods are frequently used when it is not possible to use a quantitative method or to reduce subjectivity in qualitative methods.

For example, the qualitative measure of “high” may be given a quantitative weight of 5, “medium” may be given 3 and “low” may be given 1. The total weight for the subject area that is evaluated may be the aggregate of the weights so derived for the various factors being considered.

Quantitative Analysis Methods

Quantitative analysis methods use numeric (e.g., monetary) values to describe the likelihood and impacts of risk, using data from several types of sources such as historic records, past experiences, industry practices and records, statistical theories, testing, and experiments. This is a benefit because these methods provide measurable results.

Many quantitative risk analysis methods are currently used by military, nuclear, chemical and financial entities, as well as other areas. A quantitative risk analysis is generally performed during a BIA. The main problem within this process is the valuation of information assets. Different individuals may assign different values to the same asset, depending on the relevance of information to the individuals. In the case of technology assets, it is not the cost of the asset that is considered but also the cost of replacement and the value of information processed by that asset.

2.7 MATURITY MODELS

The effectiveness and efficacy of IT governance are dependent on the quality management strategies and policies that are embedded in the IT governance framework. The integration of defined processes and corresponding process management techniques across the enterprise is related to the effectiveness and efficiency of the IS organization. Quality management strategies and policies outline how the IT strategies, policies, procedures and standards are maintained, used and improved over time as the organization changes.

Implementation of IT governance requires ongoing performance

measurement of an organization’s resources that contribute to the execution of processes that deliver IT services to the business. Maintaining consistent

efficiency and effectiveness of processes requires implementing a process maturity framework. The framework can be based on various models such as Capability Maturity Model Integration (CMMI®) and the Initiating, Diagnosing, Establishing, Acting and Learning (IDEAL) model.

The IS auditor needs to understand how the development, implementation and integration of capability and maturity modeling quality tools, techniques and processes (TTPs) will facilitate and foster the quality of enterprise IT

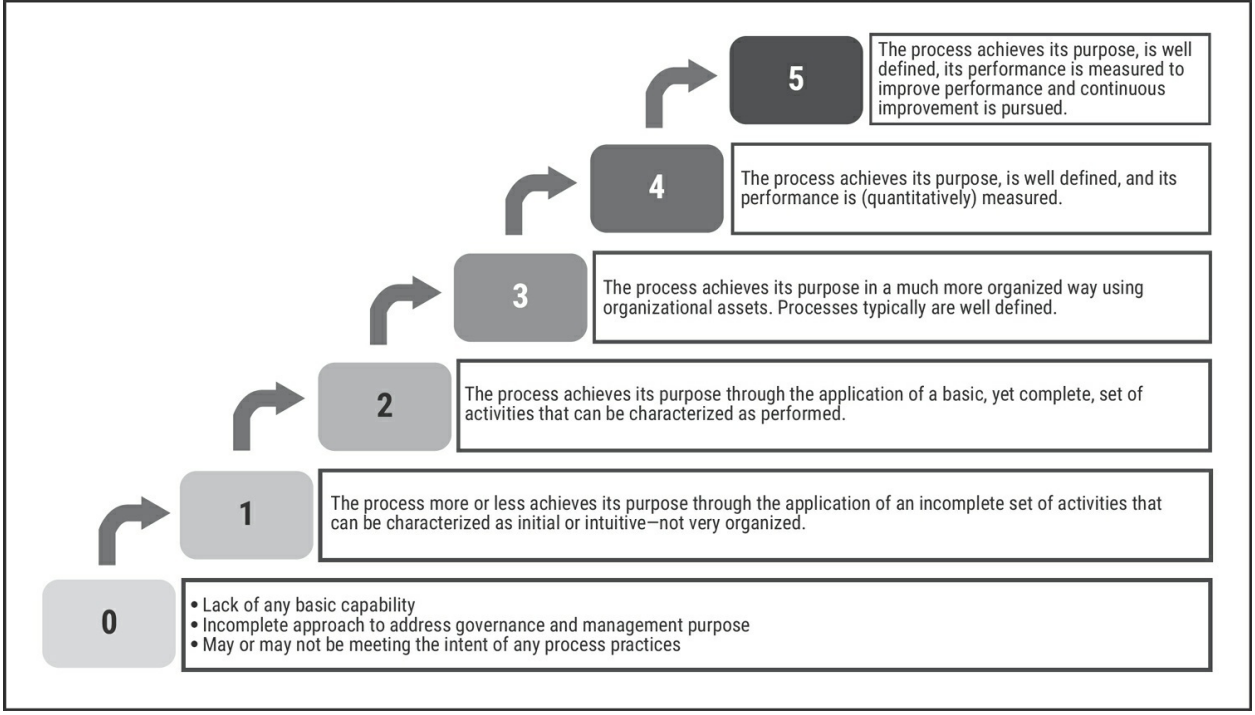
policies and procedures. These TTPs can be based on a variety of standard frameworks. The use of quality standards within an IS organization enhances the ability of the IT organization to realize greater value and mission success.

2.7.1 CAPABILITY MATURITY MODEL INTEGRATION

Following the release and successful adoption of the capability maturity model (CMM) for software, other models were developed for disciplines such as systems engineering and integrated product development. CMMI was conceived as a means of combining the various models into a set of integrated models. CMMI describes five levels of maturity, although the descriptions of what constitutes each level differ from those used in the original CMM. CMMI is considered less directly aligned with the traditional waterfall approach to development and better aligned with contemporary software development practices including:

- Iterative development
- Early definition of architecture
- Model-based design notation

Figure 2.8—Characteristics of the Maturity Levels (CMMI)



• Component-based development

• Demonstration-based assessment of intermediate development products

• Use of scalable, configurable processes

Maturity models such as CMMI are useful to evaluate management of a computer center and the development function management process and implement and measure the IT change management process.

See **figure 2.8** for characteristics of the maturity levels.

Source: CMMI Institute, *www.cmmiinstitute.com*

2.7.2 INITIATING, DIAGNOSING, ESTABLISHING,

ACTING AND LEARNING (IDEAL) MODEL

The IDEAL model is a software process improvement (SPI) program model, developed by the Software Engineering Institute (SEI) at Carnegie Mellon University. It forms an infrastructure to guide enterprises in planning and implementing an effective software process improvement program and consists

of five phases: initiating, diagnosing, establishing, acting and learning.

2.8 LAWS, REGULATIONS AND INDUSTRY STANDARDS AFFECTING THE ORGANIZATION

The complex nature of IT and global connectivity have introduced various types of risk within the organization's information life cycle—from receipt, processing, storage, transmission/distribution through destruction. In order to protect stakeholder interests, various legal and regulatory requirements have been enacted. The major compliance requirements that are considered globally recognized include protection of privacy and confidentiality of personal data, intellectual property rights and reliability of financial information.

In addition, there are some compliance requirements that are industry-specific. All of these drivers demand the development and implementation of well-maintained, timely, relevant and actionable organizational business policies, procedures and processes.

Legislative and regulatory requirements pertaining to the access and use of IT

resources, systems and data should be reviewed to assess whether the IT

organization is protecting IT assets and effectively managing associated risk.

For the CISA exam, the IS auditor must be aware of these globally recognized concepts; however, knowledge of specific legislation and regulations will not be tested.

2.8.1 GOVERNANCE, RISK AND COMPLIANCE

Governance, risk management and compliance (GRC) form an example of the growing recognition of the necessity for convergence, or assurance process integration. GRC is a term that reflects an approach that organizations can adopt to integrate these three areas. Often stated as a single business activity, GRC includes multiple overlapping and related activities within an organization, which may include internal audit, compliance programs such as the US Sarbanes-Oxley Act, ERM, operational risk, incident management and other activities.

According to Michael Rasmussen, an industry GRC analyst, the challenge in defining GRC is that, individually, each term has “many different meanings

within organizations.” Development of GRC was initially a response to the US Sarbanes-Oxley Act, but has evolved as an approach to ERM.

While a GRC program can be used in any area of an organization, it is usually focused on financial, IT and legal areas. Financial GRC is used to ensure proper operation of financial processes and compliance with regulatory requirements. In a similar fashion, IT GRC seeks to ensure proper operation and policy compliance of IT processes. Legal GRC may focus on overall regulatory compliance.

Organizations may also weigh the option of compliance to a legal or regulatory requirement and decide to accept the risk and penalties associated with noncompliance.

2.8.2 IMPACT OF LAWS, REGULATIONS AND INDUSTRY

STANDARDS ON IS AUDIT

The enterprise may be subject to audits related to specific applicable laws, regulations and industry standards. Examples of laws that may require audit include:

• United States laws:

– Financial Services Modernization Act of 1999, better known as the Gramm-Leach-Bliley Act (GLBA)

– Family Educational Rights and Privacy Act (FERPA)

– Children’s Online Privacy Protection Act (COPPA)

– Children’s Internet Protection Act (CIPA)

– Health Insurance Portability and Accountability Act (HIPAA) – The Federal Information Security Management Act of 2002 (FISMA)

• Canada’s Personal Information Protection and Electronic Documents Act

(PIPEDA)

• South Korea’s Personal Information Protection Act (PIPA)

• South Africa’s Protection of Personal Information (POPI) Act

• The UK Ministry of Defence’s (MOD) DEFCON 658

• The European Union’s GDPR

In addition, organizations operating in multiple jurisdictions must be aware of the legal and regulatory requirements in those areas in which they operate.

Some laws and regulations may apply to organizations even if they are not headquartered in the jurisdiction where the law or regulation was created. For example, GDPR applies not only to organizations within the European Union, but organizations that do business with individuals in the European Union as well.

According to The Institute of Internal Auditors, the auditor should consider the following when auditing regulatory compliance:

• **Standards and procedures**—Compliance standards and procedures should be established, which employees and other entities should follow to reduce the risk of criminal activity.

• **Assignment of responsibility to senior personnel**—Overall responsibility for compliance with standards and procedures should be assigned to specific individual(s) within senior management of the organization.

• **Reliable background of staff**—The organization should conduct background checks on staff members prior to establishing access or authority roles to ensure that such power is not delegated to individuals who have conducted illegal activity.

• **Communication of procedures**—Organizational standards and procedures should be communicated effectively to all employees and other agents via training or documentation.

• **Compliance monitoring and auditing**—The organization should take

reasonable steps to achieve compliance with its standards (e.g., monitoring and reporting).

• **Consistent enforcement**—Compliance should be enforced consistently throughout the organization, with appropriate disciplinary action taken toward offenders.

• **Appropriate response to an offense and prevention of similar offenses**

—Organizations should act appropriately (i.e., reporting to proper authorities and/or law enforcement) once an offense is detected/occurs and act to prevent future offenses in a timely manner.

PART B: IT MANAGEMENT

IT management consists of overseeing the concepts related to IT operations and resources. As previously noted, management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve enterprise objectives. IT management ensures that IT continues to support enterprise objectives.

2.9 IT RESOURCE MANAGEMENT

Each enterprise faces the challenge of using its limited resources, including people and money, to achieve its goals and objectives. When an organization invests its resources in a given effort, it incurs opportunity costs because it is unable to pursue other efforts that could bring value to the enterprise. An IS

auditor should understand an organization’s investment and allocation practices to determine whether the enterprise is positioned to achieve the greatest value from the investment of its resources.

Traditionally, when IT professionals and top managers discussed the ROI of an IT investment, they were thinking about financial benefits, which include impacts on the organization’s budget and finances (e.g., cost reductions or revenue increases). Today, business leaders also consider the nonfinancial benefits of IT investments, which include impacts on operations or mission performance and results (e.g., improved customer satisfaction, better information, shorter cycle time).

Where feasible, nonfinancial benefits should be made visible and tangible by using algorithms that transform them into monetary units to understand their impact and improve their analysis.

2.9.1 VALUE OF IT

Decision-makers make IT project selection decisions based upon the perceived value of the investment. IT's value is determined by the

relationship between what the organization will pay (costs) and what it will receive (benefits). The larger the benefit in relation to cost, the greater the value of the IT project.

IT portfolio management is distinct from IT financial management in that it has an explicitly directive, strategic goal in determining what the enterprise will invest or continue to invest in versus what the enterprise will divest.

2.9.2 IMPLEMENTING IT PORTFOLIO MANAGEMENT

IT portfolio management is a method of determining if the organization is pursuing the best IT-related projects to achieve enterprise goals. Portfolio criteria can be classified and evaluated, whether they are financial, strategic or tactical. While the criteria should be comprehensive, they also need to be able to change as the organization's strategy changes.

The first practical and necessary step for implementation is to standardize the terminology to reduce any misunderstandings. Other start-up tasks include the following:

• Ensure management commitment and agreed-upon targets.

• Plan the portfolio management model in line with the organization's management process.

• Specify portfolio inclusion criteria.

• Describe roles, tasks and decisions of those involved.

• Organize the required tools, support and instructions.

Implementation methods include risk profile analysis; diversification of projects, infrastructure and technologies; continuous alignment with business goals; and continuous improvement. Some projects are discretionary, while others are mandatory (e.g., required because of legislation). In either situation, a documented business case should be required. Completed programs should not be deleted from the portfolio—their status should be changed and results evaluated against the original plans.

IT Portfolio Management Versus Balanced Scorecard

The biggest advantage of IT portfolio management is its agility in adjusting investments. While BSCs also emphasize the use of vision and strategy in

any investment decision, the oversight and control of operations budgets is not the goal. IT portfolio management allows organizations to adjust investments based upon the built-in feedback mechanism.

2.9.3 IT MANAGEMENT PRACTICES

IT management practices reflect the implementation of policies and procedures developed for various IT-related management activities. In most organizations, the IT department is a service (support) department. The traditional role of a service department is to help production (line) departments conduct their operations more effectively and efficiently.

However, IT is an integral part of every facet of the operations of an organization and IS auditors must understand and appreciate the extent to which a well-managed IT department is crucial to achieving the

organization’s objectives.

Management activities to review the policy/procedure formulations and their effectiveness within the IT department include practices such as HR

(personnel) management, organizational change management, financial management practices and information security management.

2.9.4 HUMAN RESOURCE MANAGEMENT

HR management relates to organizational policies and procedures for recruiting,

selecting, training and promoting staff; measuring staff performance; disciplining staff; planning for succession; and retaining staff.

The effectiveness of these activities, as they relate to the IT function, impacts the quality of staff and the performance of IT duties.

Note: The IS auditor should be aware of HR management issues, but this information is not tested in the CISA exam due to its subjectivity and organization-specific subject matter.

Hiring

An organization's hiring practices are important to ensure that the most effective and efficient employees are chosen and the organization is in

compliance with legal recruitment requirements. Some of the common controls include the following:

• Background checks (e.g., criminal, financial, professional, references, qualifications)

• Confidentiality agreements or nondisclosure agreements. Specific provision may be made in these agreements to abide by the security policies of the previous employer and not to exploit the knowledge of internal controls in that organization.

• Employee bonding to protect against losses due to theft, mistakes and neglect (Note: Employee bonding is not an accepted practice all over the world; in some countries, it is not legal.)

• Conflict-of-interest agreements

• Codes of professional conduct/ethics

• Noncompete agreements

Control risk includes the following possibilities:

• Employees may not be suitable for the position they are recruited to fill.

• Reference checks may not be carried out.

• Temporary staff and third-party contractors may introduce uncontrolled risk.

• Lack of awareness of confidentiality requirements may lead to the compromise of the overall security environment.

Employee Handbook

Employee handbooks, distributed to all employees at time of hire, should explain items such as:

• Security policies and procedures

• Acceptable and unacceptable conduct

• Organizational values and ethics code

• Company expectations

• Employee benefits

• Vacation (holiday) policies

• Overtime rules

• Outside employment

• Performance evaluations

• Emergency procedures

• Disciplinary actions for:

– Excessive absence

– Breach of confidentiality and/or security

– Noncompliance with policies

In general, there should be a published code of conduct for the organization that

specifies the responsibilities of all employees.

Promotion Policies

Promotion policies should be fair and equitable and understood by employees. Policies should be based on objective criteria and consider an individual's performance, education, experience and level of responsibility.

The IS auditor should ensure that the IT organization has well-defined policies and procedures for promotion and is adhering to them.

Training

Training should be provided on a regular basis to all employees based on the areas where employee expertise is lacking. Training is particularly important for IT professionals, given the rapid rate of change in technology and products. It assures more effective and efficient use of IT resources and strengthens employee morale. Training must be provided when new hardware and/or software is being implemented. Training should also include relevant management, project management and technical training.

Cross-training means having more than one individual properly trained to perform a specific job or procedure. This practice has the advantage of decreasing dependence on one employee and can be part of succession planning. It also provides a backup for personnel in the event of absence for any reason and, thereby, provides for continuity of operations. However, in using this approach, it would be prudent to have first assessed the risk of any person knowing all parts of a system and what exposure this may cause.

Scheduling and Time Reporting

Proper scheduling provides for more efficient operation and use of computing resources. Time reporting allows management to monitor the scheduling

process. Management can then determine whether staffing is adequate and whether the operation is running efficiently. It is important that the information being entered or recorded into such a system is accurate.

Time reporting can be an excellent source of information for IT governance purposes. One of the scarcest resources in IT is time, and its proper reporting

will definitely help to better manage this finite resource. This input can be useful for cost allocation, invoicing, chargeback, key goal indicator (KGI) and KPI measurement, and activities analysis (e.g., how many hours the organization dedicates to application changes versus new developments).

Terms and Conditions of Employment

As part of their contractual obligation, employees, contractors and third-party users should agree and sign the terms and conditions of their employment, which should state their and the organization's responsibilities for information security. The terms and conditions of employment should reflect the organization's security policy in addition to clarifying and stating the following:

• The requirement for all employees, contractors and third-party users who are given access to sensitive information to sign a confidentiality or nondisclosure agreement prior to being given access to IPFs

• The employee's, contractor's and any other user's legal responsibilities and rights (e.g., regarding copyright laws or data protection legislation)

• Responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or third-party user

• Responsibilities of the employee, contractor or third-party user for the handling of information received from other companies or external parties

• Responsibilities of the organization for the handling of personal information, including personal information created as a result of, or in the course of, employment with the organization

• Responsibilities that are extended outside the organization's premises and outside normal working hours (e.g., in the case of working at home)

• Actions to be taken if the employee, contractor or third-party user disregards the organization's security requirements

The organization should ensure that employees, contractors and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated

with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.

During Employment

Management should require employees, contractors and third-party users to apply security in accordance with the established policies and procedures of the organization. Specific responsibilities should be documented in approved job descriptions. This will help ensure that employees, contractors and third-party users are aware of information security threats and concerns, as well as their responsibilities and liabilities, and they are equipped to support the organizational security policy in the course of their normal work and to reduce the risk of human error.

Management responsibilities should be defined to ensure that security is applied throughout an individual's employment within the organization. An adequate level of awareness, education and training in security procedures and the correct use of IPFs should be provided to all employees, contractors and third-party users to minimize possible security risk. A formal disciplinary process for handling security breaches should be established.

Employee Performance Evaluations

Employee assessment/performance evaluations must be a standard and regular feature for all IT staff. The HR department should ensure that IT

managers and IT employees set mutually agreed-on goals and expected results. Assessment can be set against these goals only if the process is objective and neutral.

Salary increments, performance bonuses and promotions should be based on performance. The same process can also allow the organization to gauge employee aspirations and satisfaction and identify problems.

Required Vacations

A required vacation (holiday) ensures that once a year, at a minimum, someone

other than the regular employee will perform a job function. This reduces the opportunity to commit improper or illegal acts. During this time, it may be possible to discover fraudulent activity as long as there has been no collusion between employees to cover possible discrepancies.

Job rotation provides an additional control to reduce the risk of fraudulent or malicious acts because the same individual does not perform the same tasks all the time. This provides an opportunity for an individual other than the regularly assigned person to perform the job and notice possible irregularities. In addition, job rotation also guards against the risk of overdependence on key staff by spreading experience in procedures and controls as well as specific technologies. Without this, an enterprise could be vulnerable should a key employee be unavailable.

Note: A CISA should be familiar with ways to mitigate internal fraud.

Mandatory leave is such a control measure.

Termination Policies

Written termination policies should be established to provide clearly defined steps for employee separation. It is important that policies be structured to provide adequate protection for the organization's computer assets and data.

Termination practices should address voluntary and involuntary (e.g., immediate) terminations. For certain situations, such as involuntary terminations under adverse conditions, an organization should have clearly defined and documented procedures for escorting the terminated employee from the premises. In all cases, however, the following control procedures should be applied:

• **Return of all devices, access keys, ID cards and badges**—To prevent easy physical access

• **Deletion/revocation of assigned logon IDs and passwords**—To prohibit system access

• **Notification**—To alert appropriate staff and security personnel regarding the employee's status change to "terminated"

• **Arrangement of the final pay routines**—To remove the employee from active payroll files

• **Performance of a termination interview**—To gather insight on the employee's perception of management

Note: Changes in job role and responsibilities, such as a transfer to a different department, may necessitate revocation and reissuance of system and work area access rights similar to termination procedures.

2.9.5 ORGANIZATIONAL CHANGE MANAGEMENT

Organizational change management involves use of a defined and

documented process to identify and apply technology improvements at the infrastructure and application levels that are beneficial to the organization and involve all levels of the organization impacted by the changes. This level of involvement and communication will ensure that the IT department fully understands the users' expectations and changes are not resisted or ignored by users after they are implemented.

The IT department is the focal point for such changes by leading or facilitating change in the organization. This includes staying abreast of technology changes that could lead to significant business process improvements and obtaining senior management commitment for the changes or projects that will be required at the user level.

After senior management support is obtained to move forward with the changes or projects, the IT department can begin working with each functional area and its management to obtain support for the changes. In addition, the IT department will need to develop a communication process that is directed at the end users to update them on the changes and their impact and benefit and provide a method for obtaining user feedback and involvement.

User feedback should be obtained throughout the project, including validation of the business requirements and training on and testing of the new or changed functionality.

See chapter 3, Information Systems Acquisition, Development and Implementation, for more information.

2.9.6 FINANCIAL MANAGEMENT PRACTICES

Financial management is a critical element of all business functions. In a cost-intensive computer environment, it is imperative for sound financial management practices to be in place.

The user-pays scheme, a form of chargeback, can improve application and monitoring of IS expenses and available resources. In this scheme the costs of IS services—including staff time, computer time and other relevant costs—

are charged back to the end users based on a standard (uniform) formula or calculation.

Chargeback provides all involved parties with a “marketplace” measure of the effectiveness and efficiency of the service provided by the information processing facility. Where implemented, the chargeback policy should be set forth by the board and jointly implemented by the CFO, user management and IS management.

IS Budgets

IS management, like all other departments, must develop a budget. A budget allows for forecasting, monitoring and analyzing financial information. The budget allows for an adequate allocation of funds, especially in an IS

environment where expenses can be cost-intensive. The IS budget should be linked to short- and long-range IT plans.

Software Development

In the United States and in countries using International Accounting Standards Board (IASB) guidance, accounting standards require that companies have a detailed understanding of their development efforts, including time spent on specific projects and activities. An IS auditor should understand these requirements and the practices used by companies to track software development costs.

International Accounting Standard 38 (IAS 38) outlines six criteria that must

be met if development costs are to be capitalized. Of these, an organization

should demonstrate, according to IAS 38.57.d, “how the intangible asset will generate probable future economic benefits.” Intangible assets include websites and software, if they satisfy this criterion. Interpretations of what

“demonstrating the usefulness of the intangible asset” means vary. Therefore, the IS auditor working with organizations following International Financial Reporting Standards (IFRS) will need to obtain the guidance from the chartered accountants responsible for financial reporting.

2.9.7 INFORMATION SECURITY MANAGEMENT

Information security management provides the lead role to ensure that the organization’s information and the information processing resources under its control are properly protected. This includes leading and facilitating the implementation of an organizationwide information security program that includes the development of a BIA, a BCP and a DRP related to IT

department functions in support of the organization’s critical business processes. A major component in establishing such programs is the application of risk management principles to assess the risk to IT assets, mitigate the risk to an appropriate level as determined by management and monitor the remaining residual risk.

2.10 IT SERVICE PROVIDER ACQUISITION AND MANAGEMENT

Sourcing practices relate to the way in which the organization will obtain the IT functions required to support the business. Organizations can perform all the IT functions in-house (known as “insourcing”) in a centralized fashion or outsource all functions across the globe. The sourcing strategy should consider each IT function and determine which approach allows the IT

function to meet the enterprise’s goals.

Delivery of IT functions can be characterized as:

- **Insourced**—Fully performed by the organization’s staff
- **Outsourced**—Fully performed by the vendor’s staff

• **Hybrid**—Performed by a mix of the organization's and the vendor's staffs;

can include joint ventures/supplemental staff

IT functions can be performed across the globe, taking advantage of time zones and arbitraging labor rates, and can be classified as:

• **Onsite**—Staff work onsite in the IT department.

• **Offsite**—Also known as nearshore, staff work at a remote location in the same geographic area.

• **Offshore**—Staff work at a remote location in a different geographic region.

The organization should evaluate its IT functions and determine the most appropriate method of delivering the IT functions, considering the following questions:

• Is this a core function for the organization?

• Does this function have specific knowledge, processes and staff critical to meeting its goals and objectives, which cannot be replicated externally or in another location?

• Can this function be performed by another party or in another location for the same or lower price, with the same or higher quality, and without increasing risk?

• Does the organization have experience managing third parties or using remote/offshore locations to execute IS or business functions?

• Are there any contractual or regulatory restrictions preventing offshore locations or use of foreign nationals?

On completion of the sourcing strategy, the IT steering committee should review and approve the strategy. At this point, if the organization has chosen to use outsourcing, a rigorous process should be followed, including the following steps:

• Define the IT function to be outsourced.

• Describe the service levels required and minimum metrics to be met.

• Know the desired level of knowledge, skills and quality of the expected service provider desired.

• Know the current in-house cost information to compare with third-party bids.

• Conduct due diligence reviews of potential service providers.

• Confirm any architectural considerations to meeting contractual or

regulatory requirements.

Using this information, the organization can perform a detailed analysis of the service provider bids and determine whether outsourcing will allow the organization to meet its goals in a cost-effective manner, with limited risk.

The same process should be considered when an organization chooses to globalize or take its IT functions offshore.

An IS auditor must understand the variety of vendor-provided services (e.g., commercial off-the-shelf HW/SW products, outsourced services to include cloud offerings, managed services) and the functional requirements these services are addressing. Furthermore, an IS auditor needs to understand the vendor's SLAs that are in place to address system/software operational and technical support requirements. Additional considerations also include suppliers' financial viability, licensing scalability and provisions for software escrow.

Although IS auditors are not legal or "contract auditors," they must understand the importance of requirements specifications that form the request for proposal (RFP). They must understand the need for required security and other controls to be specified, the essential elements of vendor selection to ensure that a reliable and professional vendor is chosen, and the essential contents of the contract—most notably, the need, as appropriate, for an escrow agreement to be in place. The right to audit must also be addressed in the contract. The same applies when assurance must be provided by a trusted third party (e.g., through certification on an international standard).

2.10.1 OUTSOURCING PRACTICES AND STRATEGIES

Outsourcing is the mechanism that allows organizations to transfer the delivery of services to third parties. Fundamental to outsourcing is accepting that, while service delivery is transferred, accountability remains firmly with the management of the client organization, which must ensure that the risk is properly managed and there is continued delivery of value from the service provider. Transparency and ownership of the decision-making process must reside within the purview of the client.

The decision to outsource is a strategic, not merely a procurement, decision.

The organization that outsources is effectively reconfiguring its value chain by identifying activities that are core to its business, retaining them and making noncore activities candidates for outsourcing. Understanding this in the light of governance is key, not only because well-governed organizations have been shown to increase shareholder value, but, more important, because organizations are competing in an increasingly aggressive, global and dynamic market.

Establishing and retaining competitive and market advantage require the organization to be able to respond effectively to competition and changing market conditions. Outsourcing can support this, but only if the organization understands which parts of its business truly create competitive advantage.

Outsourcing practices relate to contractual agreements under which an organization hands over control of part or all of the functions of the IT

department to an external party. Most IT departments use information resources from a wide array of vendors and, therefore, need a defined outsourcing process for effectively managing contractual agreements with these vendors.

The contractor provides the resources and expertise required to perform the agreed-on service. Outsourcing is becoming increasingly important in many organizations. The IS auditor must be aware of the various forms outsourcing can take and the associated risk.

The specific objectives for IT outsourcing vary from organization to organization. Typically, the goal is to achieve lasting, meaningful improvement in business processes and services through corporate restructuring to take advantage of a vendor’s core competencies. As with the decision to downsize or rightsize, the decision to outsource services and products requires management to revisit the control framework on which it can rely.

Reasons for embarking on outsourcing include:

• A desire to focus on core activities

• Pressure on profit margins

• Increasing competition that demands cost savings and faster time-to-market

• Flexibility with respect to organization, structure and market size An IS auditor should determine whether an enterprise considered the advantages, the disadvantages and business risk, and the risk reduction options depicted in **figure 2.9** as it developed its outsourcing practices and strategies. In addition, an enterprise should consider the following provisions in its outsourcing contracts:

• Incorporate service quality expectations, including usage of *ISO/IEC 15504*

(Software Process Improvement and Capability dEtermination [SPICE]), CMMI, ITIL or ISO methodologies.

• Ensure adequate contractual consideration of access control/security administration, whether vendor- or owner-controlled.

• Ensure that violation reporting and follow-up are required by the contract.

• Ensure any requirements for owner notification and cooperation with any investigations.

• Ensure that change/version control and testing requirements are contractually required for the implementation and production phases.

• Ensure that the parties responsible and the requirements for network controls are adequately defined and any necessary delineation of these responsibilities established.

• State specific, defined performance parameters that must be met, such as minimum processing times for transactions or minimum hold times for contractors.

Figure 2.9—Advantages, Disadvantages and Business Risk, and Risk Reduction Options Related to Outsourcing

Possible Advantages

Possible Disadvantages and

Risk Reduction Options

Business Risk

• Commercial outsourcing

• Costs exceeding customer

• Establishing measurable,

companies can achieve

expectations

partnership-enacted shared

economies of scale through

• Loss of internal IT

goals and rewards

the deployment of reusable

experience

• Software escrow to ensure

component software.

• Loss of control over IT

maintenance of the software

• Outsourcing vendors are

• Vendor failure (ongoing

• Using multiple suppliers or

likely to be able to devote

concern)

withholding a piece of

more time and to focus more

• Limited product access

business as an incentive

effectively and efficiently on

• Difficulty in reversing or

• Performing periodic

a given project than in-house

changing outsourced

competitive reviews and

staff.

arrangements

benchmarking/benchtrending

• Outsourcing vendors are

• Deficient compliance with

• Implementing short-term

likely to have more

legal and regulatory

contracts

experience with a wider array

requirements

• Forming a cross-functional

of problems, issues and

• Contract terms not being met

contract management team

techniques than in-house

• Lack of loyalty of contractor

• Including contractual

staff.

personnel toward the

provisions to consider as

• The act of developing

customer

many contingencies as can

specifications and contractual

• Disgruntled

reasonably be foreseen

agreements using

customers/employees as a

outsourcing services is likely

result of the outsource

to result in better

arrangement

specifications than if

• Service costs not being

developed only by in-house

competitive over the period

staff.

of the entire contract

• Because vendors are highly

• Obsolescence of vendor IT

sensitive to time-consuming

systems

diversions and changes,

• Failure of either company to

feature creep or scope creep

receive the anticipated

is substantially less likely

benefits of the outsourcing

with outsourcing vendors.

arrangement

• Reputational damage to

either or both companies due

to project failures

• Lengthy, expensive litigation

• Loss or leakage of

information or processes

• Incorporate capacity management criteria.

• Provide contractual provisions for making changes to the contract.

• Provide a clearly defined dispute escalation and resolution process.

• Ensure that the contract indemnifies the company from damages caused by the organization responsible for the outsourced services.

• Require confidentiality agreements protecting both parties.

• Incorporate clear, unambiguous “right to audit” provisions, providing the right to audit vendor operations (e.g., access to facilities, access to records, right to make copies, access to personnel, provision of computerized files) as they relate to the contracted services.

• Ensure that the contract adequately addresses business continuity and disaster recovery provisions and appropriate testing.

• Establish that the confidentiality, integrity and availability (sometimes

referred to as the CIA triad) of organization-owned data must be maintained, and clearly establish the ownership of the data.

• Require that the vendor comply with all relevant legal and regulatory requirements, including those enacted after contract initiation.

• Establish ownership of intellectual property developed by the vendor on behalf of the customer.

• Establish clear warranty and maintenance periods.

• Provide software escrow provisions.

• Protect intellectual property rights.

• Comply with legislation.

• Establish clear roles and responsibilities between the parties.

• Require that the vendor follow the organization's policies, including its information security policy, unless the vendor's policies have been agreed to in advance by the organization.

• Require the vendor to identify all subcontract relationships and requiring the organization's approval to change subcontractors.

Outsourcing requires management to actively manage the relationship and the outsourced services. Because the outsourcing agreement is governed by the contract terms, the contract with the outsourced service provider should include a description of the means, methods, processes and structure accompanying the offer of IT services and products, and the control of quality. The formal or legal character of these agreements depends on the relationship between the parties and the demands placed by principals on those performing the engagement.

After the outsourcer has been selected, the IS auditor should regularly review the contract and service levels to ensure that they are appropriate. In addition, the IS auditor could review the outsourcer's documented procedures and results of their quality programs—including ISO/IEC 15504 (SPICE), CMMI, ITIL and ISO methodologies. These quality programs require regular audits to certify that the process and procedures meet the quality standard.

Outsourcing is not only a cost decision; it is a strategic decision that has significant control implications for management. Quality of service, guarantees of continuity of service, control procedures, competitive

advantage and technical knowledge are issues that need to be part of the decision

to outsource IT services. Choosing the right supplier is extremely important, particularly when outsourcing is a long-term strategy. The compatibility of suppliers in terms of culture and personnel is an important issue that should not be overlooked by management.

The decision to outsource a particular service currently within the organization demands proper attention to contract negotiations. A well-balanced contract and SLA are of great importance for quality purposes and future cooperation between the concerned parties.

SLAs stipulate and commit a vendor to a required level of service and support options. This includes providing for a guaranteed level of system performance regarding downtime or uptime and a specified level of customer support. Software or hardware requirements are also stipulated. SLAs also provide for penalty provisions and enforcement options for services not provided and may include incentives such as bonuses or gain-sharing for exceeding service levels.

SLAs are a contractual means of helping the IT department manage information resources that are under the control of a vendor. Above all, an SLA should serve as an instrument of control. If the outsourcing vendor is from another country, the organization should be aware of cross-border legislation.

Industry Standards/Benchmarking

Most outsourcing organizations must adhere to a well-defined set of standards that can be relied on by their clients. These industry standards provide a means of determining the level of performance provided by similar IPF environments. These standards can be obtained from vendor user groups, industry publications and professional associations. Examples include *ISO*

9001:2015: Quality management systems—Requirements and CMMI.

Globalization Practices and Strategies

Many organizations have chosen to globalize their IT functions in addition to outsourcing functions. The globalization of IT functions is performed for

many of the same reasons cited for outsourcing; however, the organization may choose not to outsource the function. Globalizing IT functions requires management to actively oversee the remote or offshore locations.

Where the organization performs functions in-house, it may choose to move the IT functions offsite or offshore. The IS auditor can assist in this process by ensuring that IT management considers the following risk and audit concerns when defining the globalization strategy and completing the subsequent transition to remote offshore locations:

• **Legal, regulatory and tax issues**—Operating in a different country or region may introduce new risk about which the organization may have limited knowledge.

• **Continuity of operations**—Business continuity and disaster recovery may not be adequately provided for and tested.

• **Personnel**—Needed modifications to personnel policies may not be considered.

• **Telecommunication issues**—Network controls and access from remote or offshore locations may be subject to more frequent outages or a larger number of security exposures.

• **Cross-border and cross-cultural issues**—Managing people and processes across multiple time zones, languages and cultures may present unplanned challenges and problems. Cross-border data flow may also be subject to legislative requirements (e.g., that data must be encrypted during transmission).

• **Planned globalization and/or important expansion**

2.10.2 OUTSOURCING AND THIRD-PARTY AUDIT REPORTS

One method for the IS auditor to have assurance of the controls implemented by a service provider requires the provider to periodically submit a third-party audit report. These reports cover the range of issues related to confidentiality, integrity and availability of data. In some industries, third-party audits may fall under regulatory oversight and control, such as Statement on Standards for Attestation Engagements (SSAE) 18 and an audit guide by the American Institute of Certified Public Accountants (AICPA),

which provides a framework for three Service Organization Control (SOC)

reporting options (SOC 1, SOC 2 and SOC 3 reports). These reporting standards represent significant changes from the Statement on Auditing Standards (SAS) 70 report, as organizations increasingly became interested in risk beyond financial statement reporting (e.g., privacy). The International Auditing and Assurance Standards Board (IAASB) also issued new guidance in this regard—the International Standard on Assurance Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization.

An IS auditor should be familiar with the following:

• Management assertions and how well these address the services being provided by the service provider

• SSAE 18 reports as follows:

– SOC 1: Report on the service organization's system controls likely to be relevant to user entities' internal control over financial reporting

– SOC 2: Report on the service organization's system controls relevant to security, availability, processing integrity, confidentiality or privacy, including the organization's compliance with its privacy practices

– SOC 3: Similar to a SOC 2 report, but does not include the detailed understanding of the design of controls and the tests performed by the service auditor

• Additional third-party audit reports such as penetration tests and security assessments. Note: Third-party assessments should be performed by independent, objective and competent third parties.

• How to obtain the report, review it and present results to management for further action

2.10.3 CLOUD GOVERNANCE

The strategic direction of the business and of IT in general is the main focus when considering the use of cloud computing. As enterprises look to the cloud to provide IT services that traditionally have been managed internally, they will need to make some changes to help ensure that they continue to meet performance objectives, their technology provisioning and business are

strategically aligned, and risk is managed. Ensuring that IT is aligned with the business, systems are secure, and risk is managed is challenging in any

environment and even more complex in a third-party relationship. Typical governance activities such as goal setting, policy and standard development, defining roles and responsibilities, and managing risk must include special considerations when dealing with cloud technology and its providers.

As with all organizational changes, it is expected that some adjustments will need to be made to the way business processes are handled. Business/IT

processes such as data processing, development and information retrieval are examples of potential change areas. Additionally, processes detailing the way information is stored, archived and backed up will need revisiting.

The cloud presents many unique situations for businesses to address. One large governance issue is that business unit personnel, who were previously forced to go through IT for service, can now bypass IT and receive service directly from the cloud. Policies must be modified or developed to address the process of sourcing, managing and discontinuing the use of cloud services.

The responsibility for managing the relationship with a third party should be assigned to a designated individual or service management team. In addition, the organization should ensure that the third party assigns responsibilities for checking for compliance and enforcing the requirements of the agreements.

Sufficient technical skills and resources should be made available to monitor whether requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organization should maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or IPFs accessed, processed or managed by a third party. The organization also should ensure that it retains visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting/response through a clearly defined reporting process, format and structure. When outsourcing, the organization needs to be aware that the ultimate responsibility for information processed by an outsourcing party remains with the organization.

Note: Technical aspects of cloud computing and cloud computing delivery models are discussed in chapter 5, Protection of Information Assets.

2.10.4 GOVERNANCE IN OUTSOURCING

Governance of outsourcing is the set of responsibilities, roles, objectives, interfaces and controls required to anticipate change and manage the introduction, maintenance, performance, costs and control of third-party-provided services. It is an active process that the client and service provider must adopt to provide a common, consistent and effective approach that identifies the necessary information, relationships, controls and exchanges among many stakeholders across both parties.

The decision to outsource and subsequently successfully manage that relationship demands effective governance. Most people who conduct outsourcing contracts include basic control and service execution provisions; however, one of the main objectives of the outsourcing governance process, as defined in the outsourcing contract, is to ensure continuity of service at the appropriate levels, profitability and added value to sustain the commercial viability of both parties. Experience has shown that many companies make assumptions about what is included in the outsource proposition. Whereas it is neither possible nor cost-effective to contractually define every detail and action, the governance process provides the mechanism to balance risk, service demand, service provision and cost.

The governance of outsourcing extends both parties' (i.e., client and supplier) responsibilities into the following:

• Ensure contractual viability through continuous review, improvement and benefit gain to both parties.

• Include an explicit governance schedule to the contract.

• Manage the relationship to ensure that contractual obligations are met through SLAs and operating level agreements (OLAs).

• Identify and manage all stakeholders, their relationships and expectations.

• Establish clear roles and responsibilities for decision making, issue escalation, dispute management, demand management and service

delivery.

• Allocate resources, expenditures and service consumption in response to prioritized needs.

• Continuously evaluate performance, cost, user satisfaction and effectiveness.

• Communicate across all stakeholders on an ongoing basis.

The increasing size of the technology solution space is driven by the pace of technological evolution. Acquiring, training and retaining qualified staff are becoming more expensive. Investing in costly technology implementation and training is seen as less of an organizational core activity than is the ability to work effectively across the value chain by integrating the outsourcing of services where appropriate.

Although the term “business alignment” is often used, what it encompasses is not always clear. In the widest sense, it involves making the services provided by the corporate IT function more closely reflect the requirements and desires of the business users. When organizations recognize what is core to their business and which services provide them differential advantage, and then outsource the activities that support these services, business alignment can be achieved. If the degree to which this alignment is approached is to be understood, the implication is that SLAs and OLAs must be established, monitored and measured in terms of performance and user satisfaction.

Business alignment should be driven by the service end user.

Governance should be preplanned and built into the contract as part of the service cost optimization. The defined governance processes should evolve as the needs and conditions of the outsourcing relationship adapt to changes to service demand and delivery and to technology innovation.

It is critical for the IS auditor to understand right-to-audit clauses and controls in outsourcing activities involving confidential information and sensitive processes. This understanding includes, but is not limited to these issues:

• How auditing of the outsourced service provider is allowed to be conducted under the terms of the contract

• What visibility the IS auditor has into the internal controls being implemented by the outsourced service provider to provide reasonable

assurance that confidentiality, integrity and availability and preventive, detective and corrective controls are in place and effective

• Requirement that SLAs regarding problem management including incident response are documented and communicated to all parties affected by these outsourcing agreements

2.10.5 CAPACITY AND GROWTH PLANNING

Given the strategic importance of IT in companies and the constant change in technology, capacity and growth planning are essential. This activity must be reflective of the long- and short-range business plans and must be considered within the budgeting process. Changes in capacity should reflect changes in the underlying infrastructure and in the number of staff available to support the organization. A lack of appropriately qualified staff may delay projects that are critical to the organization or result in not meeting agreed-on service levels. This can lead some organizations to choose outsourcing as a solution for growth.

2.10.6 THIRD-PARTY SERVICE DELIVERY

MANAGEMENT

Every organization using the services of third parties should have a service delivery management system in place to implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements.

The organization should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed to with the third party.

2.10.7 MONITORING AND REVIEW OF THIRD-PARTY

SERVICES

The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.

Monitoring and review of third-party services should ensure that the information security terms and conditions of the agreements are being adhered to, and information security incidents and problems are managed

properly. This should involve a service management relationship and process between the organization and the third party to accomplish the following:

• Monitor service performance levels to check adherence to the agreements.

• Review service reports produced by the third party and arrange regular progress meetings as required by the agreements.

• Provide information about information security incidents and review of this information by the third party and the organization, as required by the agreements and any supporting guidelines and procedures.

• Review third-party audit trails and records of security events, operational problems, failures, tracing of faults, and disruptions related to the service delivered.

• Resolve and manage any identified problems.

2.10.8 MANAGING CHANGES TO THIRD-PARTY

SERVICES

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed considering the criticality of business systems and processes involved and reassessing risk.

The process of managing changes to a third-party service needs to consider:

• Changes made by the organization to implement:

– Enhancements to the current services offered

– Development of any new applications and systems

– Modifications or updates of the organization’s policies and procedures

– New controls to resolve information security incidents and improve security

– Updates to policies, including the IT security policy

• Changes in third-party services to implement:

– Changes and enhancements to networks

– Use of new technologies

– Adoption of new products or newer versions/releases

– New development tools and environments

• Changes to physical location of service facilities

• Change of vendors or subcontractors

Service Improvement and User Satisfaction

SLAs set the baseline by which outsourcers perform the IT function. In addition, organizations can set service improvement expectations into the contracts with associated penalties and rewards. Examples of service improvements include:

• Reductions in the number of help desk calls

• Reductions in the number of system errors

• Improvements to system availability

Service improvements should be agreed on by users and IT with the goals of improving user satisfaction and attaining business objectives. User satisfaction should be monitored by interviewing and surveying users.

2.11 IT PERFORMANCE MONITORING AND REPORTING

Enterprises are making increasingly significant investments in IT and related technology. This results in high expectations by stakeholders who need to be assured that these investments are strategically aligned, managed appropriately and focused on achieving business goals.

Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, systematic and timely reporting of performance, and prompt action upon discovery of deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.

Control over monitoring that satisfies the business requirement for IT to be transparent and respect costs, benefits, strategy, policies and service levels aligned with governance requirements is achieved by the following actions:

• Collate and translate process performance reports into management reports.

• Review performance against agreed-upon targets and initiate appropriate remedial action.

This can be measured by:

• Satisfaction of management and the governance entity with the performance reporting

• Number of improvement actions driven by monitoring activities

• Percent of critical processes monitored

Enterprises that want to effectively monitor the activities of IT to ensure they are aligned with the overall business goals often use KPIs. These measurement metrics help monitor achievements compared to goals, and they help evaluate the effectiveness and efficiency of business processes. Metrics describe a quality and require a measurable baseline. They are essential tools that enable enterprises to better allocate and manage resources. They also influence and help improve business decision-making in areas such as budgets, priorities, resourcing and activities.

Developing performance metrics usually involves three steps:

• Establish critical processes to meet customer requirements.

• Identify specific, quantifiable outputs of work from the identified processes.

• Establish targets against which results can be scored.

For a metric to be considered effective, it should be consistently measured; the data should be easy to gather; it should be expressed as a number, percentage or a unit of measure; and it should be contextually specific. In addition, it should be based on acceptable good practices, be useful for internal and external comparison, and be meaningful to IT's customers and sponsors.

An IS auditor should ensure that performance metrics cover:

• Business contribution including, but not limited to, financials

• Performance against the strategic business and IT plan

• Risk and compliance with regulations

• Internal and external user satisfaction with service levels

• Key IT processes, including solution and service delivery

• Future-oriented activities (e.g., emerging technology, reusable infrastructure, business and IT personnel skill sets)

Most enterprises need to continuously monitor the performance and capacity of IT resources to ensure that regular reviews are done of the performance

measurement approach and are revised or updated according to management feedback and/or changing business needs.

2.11.1 PERFORMANCE OPTIMIZATION

Performance is not how well a system works; performance is the service perceived by users and stakeholders. Performance optimization is the process of both improving perceived service performance and improving information system productivity to the highest level possible without unnecessary additional investment in the IT infrastructure.

Within the foundation of effective performance management approaches, measures are not just used for assigning accountabilities or complying with reporting requirements. Measures are used to create and facilitate action to improve performance and, therefore, EGIT.

A performance measurement process is also required to help ensure that performance is monitored consistently and reliably. Effective governance significantly enables overall performance optimization and is achieved when:

• Goals are set from the top down and aligned with high-level, approved business goals.

• Metrics are established from the bottom up and aligned in a way that enables the achievement of goals at all levels to be monitored by each layer of management.

Critical Success Factors

Two critical governance success factors (enabling overall performance optimization) are:

• The approval of goals by stakeholders

• The acceptance of accountability for achievement of goals by management IT is a complex and technical topic; therefore, it is important to achieve transparency by expressing goals, metrics and performance reports in language meaningful to the stakeholders so that appropriate actions can be taken.

Methodologies and Tools

A variety of improvement and optimization methodologies are available that complement simple, internally developed approaches. These include:

• Continuous improvement methodologies, such as the plan-do-check-act (PDCA) cycle

• Comprehensive best practices, such as ITIL

• Frameworks, such as COBIT

PDCA is an iterative four-step management method used in business for the control and continuous improvement of processes and products. The steps in each successive PDCA cycle are:

• **Plan**—Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the specification are also a part of the targeted improvement. When possible, start on a small scale to test possible effects.

• **Do**—Implement the plan, execute the process and make the product.

Collect data for charting and analysis in the following check and act steps.

• **Check**—Study the actual results (measured and collected in the do step) and compare against the expected results (targets or goals from the plan step) to ascertain any differences. Look for deviation in implementation from the plan, and for the appropriateness/completeness of the plan to enable the execution (i.e., the do step). Charting data can make it much easier to see trends over several PDCA cycles and to convert the collected data into information, which is needed for the next step.

• **Act**—Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes.

Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve, with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

Using PDCA following agile development allows for reassessment of the direction of the project at points throughout the development life cycle. This is done through sprints or iterations, which require working groups to produce a functional product. This focus on abbreviated work cycles has led

to the description of agile methodology as iterative and incremental. As compared to a single opportunity to achieve each aspect of a project, as in the waterfall method, agile development allows for each aspect to be continually revisited.

2.11.2 TOOLS AND TECHNIQUES

Tools and techniques that facilitate measurements, good communication and organizational change include:

- Six Sigma
- IT BSC
- KPI
- Benchmarking
- Business process reengineering (BPR)
- Root cause analysis
- Life cycle cost-benefit analysis

Six Sigma and **Lean Six Sigma** are proven quantitative (data-driven) process analysis and improvement approaches that easily apply to IT. Six Sigma's objective is the implementation of a measurement-oriented strategy focused on process improvement and defect reduction. A Six Sigma defect is defined as anything outside customer specifications.

Lean Six Sigma is similar, but also seeks to eliminate unnecessary steps that do not add value.

The **IT BSC** is a management evaluation technique that can be applied to EGIT in assessing IT functions and processes.

A **KPI** is a measure that determines how well the process is performing in enabling the goal to be reached. It is a lead indicator of whether a goal will likely be reached and a good indicator of capabilities, practices and skills. For example, a service delivered by IT is a goal for IT, but a performance indicator and a capability for the business. This is why performance indicators are sometimes referred to as performance drivers, particularly in BSCs.

As controls are selected for implementation, criteria should also be established to determine the operational level and effectiveness of the controls. These criteria will often be based on KPIs that indicate whether a control is functioning correctly. For example, a KPI for the implementation process measures the relative success of the changeover compared to desired performance objectives. Success of a changeover is often measured as a percentage of errors, number of trouble reports, duration of system outage or degree of customer satisfaction. The use of the KPI indicates to management whether the change control process was managed correctly, with sufficient levels of quality and testing.

Benchmarking is a systematic approach to comparing enterprise performance against peers and competitors in an effort to learn the best ways of conducting business. Examples include benchmarking of quality, logistic efficiency and various other metrics.

BPR is the thorough analysis and significant redesign of business processes and management systems to establish a better-performing structure that is more responsive to the customer base and market conditions, while yielding material cost savings.

IT performance measurement and reporting may be a statutory or contractual requirement. Appropriate performance measurement practices for the enterprise include outcome measures for business value, competitive advantage and defined performance metrics that show how well IT performs.

Incentives, such as rewards, compensation and recognition, should be linked to performance measures. It is also important to share results and progress with employees, customers and stakeholders.

Root cause analysis is the process of diagnosis to establish the origins of events (root causes). Once identified, the root causes can then be used to develop needed controls to accurately address these root causes that lead to system

failures and deficiencies. Furthermore, root cause analysis also enables an organization to learn from consequences, typically from errors and problems, in the effort to not repeat undesired actions or results.

Life cycle cost-benefit analysis is the assessment of the following elements to determine strategic direction for IT enterprise systems and overall IT

portfolio management. These include the following:

• Life cycle (LC): A series of stages that characterize the course of existence of an organizational investment (e.g., product, project, program)

• Life cycle cost (LCC): The estimated costs of maintenance/updates, failure, and maintaining interoperability with mainstream and emerging

technologies

• Benefit analysis (BA): The user costs (or benefits) and business operational costs (or benefits) derived from the information system(s)

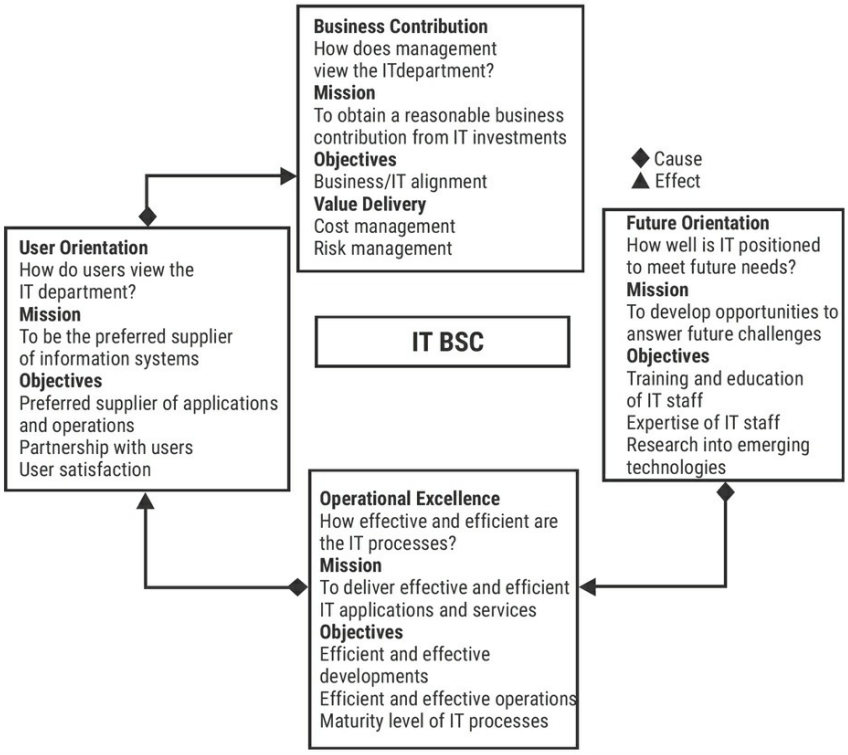
IT Balanced Scorecard

The IT BSC, **figure 2.10,** is a process management evaluation technique that can be applied to the EGIT process in assessing IT functions and processes.

The technique goes beyond the traditional financial evaluation,

supplementing it with measures concerning customer (user) satisfaction, internal (operational) processes and the ability to innovate. These additional measures drive the organization toward optimal use of IT, which is aligned with the organization’s strategic goals, while keeping all evaluation-related perspectives in balance.

Figure 2.10—Generic IT Balanced Scorecard



Source: ISACA, *IT Governance Domain Practices and Competencies: Measuring and Demonstrating the Value of IT*, USA, 2005, figure 7

To apply the BSC to IT, a multilayered structure (determined by each organization) is used in addressing four perspectives:

• **Mission**—For example:

– Become the preferred supplier of information systems.

– Deliver economic, effective and efficient IT applications and services.

– Obtain a reasonable business contribution from IT investments.

– Develop opportunities to answer future challenges.

• **Strategies**—For example:

– Develop superior applications and operations.

– Develop user partnerships and greater customer services.

– Provide enhanced service levels and pricing structures.

– Control IT expenses.

– Provide business value to IT projects.

– Provide new business capabilities.

– Train and educate IT staff and promote excellence.

– Provide support for research and development.

• **Measures**—For example:

– Provide a balanced set of metrics (i.e., KPIs) to guide business-oriented IT decisions.

• **Sources**—For example:

– End-user personnel (specific by function)

– COO

– Process owners

Use of an IT BSC is one of the most effective means to aid the IT strategy committee and management in achieving IT governance through proper IT

and business alignment. The objectives are to establish a vehicle for management reporting to the board; foster consensus among key stakeholders about IT's strategic aims; demonstrate the effectiveness and added value of IT; and communicate IT's performance, risk and capabilities.

2.12 QUALITY ASSURANCE AND QUALITY

MANAGEMENT OF IT

The integrity and reliability of enterprise IT processes are directly attributed to the QA processes in place and integrated within the enterprise. The QA program

and respective policies, procedures and processes are encompassed within a planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements.

The IS auditor needs to understand the QA and quality management concepts, structures, and roles and responsibilities within the organization.

2.12.1 QUALITY ASSURANCE

QA personnel verify that system changes are authorized, tested and implemented in a controlled manner prior to being introduced into the production environment according to a company's change and release management policies. With the assistance of source code management software (see section 4.7.7, Source Code Management), personnel also oversee the proper maintenance of program versions and source code to object integrity.

The terms "quality assurance" and "quality control" are often used interchangeably to refer to ways of ensuring the quality of a service or product. The terms, however, do have different meanings.

Quality assurance personnel usually perform two distinct tasks:

• **Quality assurance (QA)**—A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. QA helps the IT department to ensure that personnel are following prescribed quality processes. For example, QA will set up procedures (e.g., ISO 9001-compliant) to facilitate widespread use of quality management/assurance practices.

• **Quality control (QC)**—The observation techniques and activities used to fulfill requirements for quality. QC is responsible for conducting tests or reviews to verify and ensure that software is free from defects and meets user expectations. This could be done at various stages of the development of an application system, but it must be done before the programs are moved into production. For example, QC will help to ensure that programs and documentation adhere to the standards and naming conventions.

The QA function within an organization is in charge of developing, promulgating and maintaining standards for the IT function. They also provide training in QA

standards and procedures. The QC group assists by periodically checking the accuracy and authenticity of the input, processing and output of various applications.

To enable the QA function to play an effective role, the QA group should be independent within the organization. In some organizations this function may be a part of the larger control entity. In smaller organizations it may not be possible to have a separate QA function, in which case individuals may possess more than one role. However, under no circumstances should an individual review his/her own work. Additionally, the review should not be performed by an individual whose role would create a SoD conflict (e.g., a database administrator performing quality review of application system changes that would impact the database).

2.12.2 QUALITY MANAGEMENT

Quality management is one of the means by which IT department-based processes are controlled, measured and improved. Processes in this context are defined as a set of tasks that, when properly performed, produce the desired results. Areas of control for quality management may include:

- Software development, maintenance and implementation
- Acquisition of hardware and software
- Day-to-day operations
- Service management
- Security
- HR management
- General administration

The development and maintenance of defined and documented processes by the IT department are evidence of effective governance of information resources. Insistence on the observance of processes and related process management techniques is key to the effectiveness and efficiency of the IT

organization. Various standards have emerged to assist IT organizations in achieving these results. Quality standards are increasingly being used to assist IT organizations in achieving an operational environment that is predictable, measurable, repeatable and certified for their IT resources.

CASE STUDY

An IS auditor was asked to review alignment between IT and business goals for Accenco, a small, but rapidly growing, financial institution. The IS

auditor requested information including business goals and objectives and IT

goals and objectives; however, these were limited to a short, bulleted list for business goals and PowerPoint slides used in reporting meetings for IT goals.

It was also found in the documentation provided that over the past two years, the risk management committee (composed of senior management) met on only three occasions, and no minutes of what was discussed were kept for these meetings. When the IT budget for the upcoming year was compared to the strategic plans for IT, it was noted that several of the initiatives mentioned in the plans for the upcoming year were not included in the budget for that year.

The IS auditor also discovered that Accenco does not have a full-time CIO.

The organizational chart of the entity denotes an IS manager reporting to the CFO, who, in turn, reports to the board of directors. The board plays a major role in monitoring IT initiatives in the entity and the CFO communicates on a frequent basis the progress of IT initiatives.

From reviewing the SoD matrix, it is apparent that application programmers are required to obtain approval from only the DBA to directly access production data. It is also noted that the application programmers have to provide the developed program code to the program librarian, who then migrates it to production. IS audits are carried out by the internal audit department, which reports to the CFO at the end of every month, as part of business performance review process; the financial results of the entity are reviewed in detail and signed off by the business managers for correctness of data contained therein.

1.

Which of the following should be of **GREATEST** concern to the IS

auditor related to Accenco’s IT business strategy?

A. Strategy documents are informal and incomplete.

B. The risk management committee seldom meets and does not keeps minutes.

C. Budgets do not appear adequate to support future IT investments.

D. There is no full-time CIO.

2.

Which of the following would be the **MOST** significant issue to address related to Accenco’s IT business strategy?

A. The behavior related to the application programmers’ access and migration code

B. The lack of IT policies and procedures

C. The risk management practices as compared to peer organizations D. The reporting structure for IT

3.

Given the circumstances described, what would be of **GREATEST**

concern from an IT governance perspective?

A. The organization does not have a full-time CIO.

B. The organization does not have an IT steering committee. C. The board of directors plays a major role in monitoring IT initiatives.

D. The information systems manager reports to the CFO.

4.

Given the circumstances described, what would be of **GREATEST**

concern from a SoD perspective?

A. Application programmers are required to obtain approval only from the DBA for direct-write access to data.

B. Application programmers are required to turn over the developed program code to the program librarian for migration to production.

C. The internal audit department reports to the CFO.

D. Business performance reviews are required to be signed off only by the business managers.

5.

Which of the following would **BEST** address data integrity from a mitigating control standpoint?

A. Application programmers are required to obtain approval from

DBA for direct access to data.

B. Application programmers are required to hand over the developed program codes to the program librarian for transfer to production.

C. The internal audit department reports to the CFO.

D. Business performance results are required to be reviewed and

signed off by the business managers.

6.

As this is a small organization, assume the CFO performs the CIO role.

What should an IS auditor suggest regarding the governance structure?

7.

The IS budgeting process should be integrated with business processes and aligned with organizational budget cycles. What advice would an IS auditor give

to the organization to ensure the budget covers all aspects and can be accepted by the board?

8.

The internal auditor is reporting to CFO, who is the owner of IT

initiatives and operations. The reporting relationship inhibits the auditor's independence. What compensating controls could be enabled have to improve the audit efforts?

ANSWERS TO CASE STUDY QUESTIONS

1.

A.

Without explicit strategy documents, IT loses sight of the

business's direction, which, in turn, makes project selection harder and service levels difficult to define. Overall, IT

becomes suboptimal in delivery and value realization.

B.

The risk management committee's failure to hold regular

meetings and produce good documentation implies a lack of good

risk governance. Risk follows, when setting the business and IT

objectives.

C.

While an inadequate budget for future IT investments raises

concern, this is not as important as an incomplete strategy.

D.

The lack of a full-time CIO may be a concern, but it is not as important as an incomplete strategy.

2.

A.

The behavior related to application programmers' access and migration code is representative of a lack of IT policies and procedures.

B.

The lack of IT policies and procedures makes IT-related work inconsistently delivered. The policy reflects management's intentions and norms set by the strategy. The procedures are instrumental to day-to-day IT delivery.

C.

Risk management practices do not have to compare to peer organizations.

D.

While the reporting structure for IT is important, it is not as critical as IT policies and procedures.

3.

A.

Not having a full-time CIO may be a concern, but it not as

concerning as the information systems manager reporting to the

CFO.

B.

The lack of an IT steering committee may cause issues, but it is not as big a concern as the information systems manager

reporting to the CFO.

C.

The board of directors playing a major role in IT initiatives is not the major concern.

D.

The IS manager should ideally report to the board of

directors or the CEO to provide a sufficient degree of

independence. The reporting structure that requires the IS

manager to report to the CFO is not a desirable situation and could lead to compromise of certain controls.

4.

A.

The application programmers should obtain approval from

the business owners before accessing data. DBAs are only custodians of the data and should provide only the access that is authorized by the data owner.

B.

While this may be an issue, it is not as big a SoD concern as the DBA approving direct-write access.

C.

The internal audit department reporting to the CFO is not as big a SoD concern as the DBA approving direct-write access.

D.

This would not be as big a SoD concern as the DBA approving

direct-write access.

5.

A.

This would not best mitigate tampering with data.

B.

Handing over program code to the program librarian would not

best mitigate tampering with data.

C.

The reporting structure does not mitigate data tampering.

D.

Sign-off on data contained in the financial results by the

business managers at the end of the month would detect any

significant discrepancies that could result from tampering of data through inappropriate direct access of the data gained

without the approval or knowledge of the business managers.

6.

Possible answer: The CFO may act as the CIO in a small organization.

It is better to have the internal control department report to a different executive (e.g., HR or risk management). The governance function should exist to carry out the IT strategy committee's and IT steering committee's direction. SoD should be maximized to the degree

possible. Compensating controls such as supervisory review or peer review can be applied to current controls.

7.

Possible answer: An IT budgeting and investment process should be defined, and it should align with Accenco's enterprise cycles (e.g., fiscal year, quarterly reviews). The financial management process should include budgeting activity that states what budgeting approach it uses, the cost structure following the chart of accounts and the approval chain. The business case process should be used to justify the process

and persuade the board to approve it.

8.

Possible answer: In this case, the internal auditor should seek further assurance (e.g., monitoring of IS controls by tools, benchmarking efforts by the procurement team, *ad hoc* external auditing or senior management review from the board).

Chapter 3:

Information Systems Acquisition,

Development and Implementation

Overview

Domain 3 Exam Content Outline

Learning Objectives/Task Statements

Suggested Resources for Further Study

Self-assessment Questions

Answers to Self-assessment Questions

Part A: Information Systems Acquisition and Development

3.0

Introduction

3.1

Project Governance and Management

3.2

Business Case and Feasibility Analysis

3.3

System Development Methodologies

3.4

Control Identification and Design

Part B: Information Systems Implementation

3.5

Testing Methodologies

3.6

Configuration and Release Management

3.7

System Migration, Infrastructure Deployment and Data

Conversion

3.8

Post-implementation Review

Case Study

Case Study

Answers to Case Study Questions

OVERVIEW

This chapter on information systems acquisition, development and implementation provides an overview of key processes and methodologies used by organizations when creating and changing application systems and infrastructure components.

This domain represents 12 percent of the CISA examination (approximately 18 questions).

DOMAIN 3 EXAM CONTENT OUTLINE

Part A: Information Systems Acquisition and Development

1. Project Governance and Management

2. Business Case and Feasibility Analysis

3. System Development Methodologies

4. Control Identification and Design

Part B: Information System Implementation

1. Testing Methodologies

2. Configuration and Release Management

3. System Migration, Infrastructure Deployment and Data Conversion 4. Post-implementation Review

LEARNING OBJECTIVES/TASK STATEMENTS

Within this domain, an IS auditor should be able to:

• Evaluate whether the business case for proposed changes to information systems meet business objectives. (T14)

• Evaluate the organization's project management policies and practices.

(T16)

• Evaluate controls at all stages of the information systems development life cycle. (T17)

• Evaluate the readiness of information systems for implementation and migration into production. (T18)

• Conduct post-implementation review of systems to determine whether project deliverables, controls and requirements are met. (T19)

• Evaluate change, configuration, release, and patch management policies and practices. (T27)

SUGGESTED RESOURCES FOR FURTHER STUDY

ISACA, *ISACA IS Audit Basics, www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/Pages/is-audit-basics.aspx*

ISACA, *White papers, www.isaca.org/Knowledge-Center/Research/Pages/White-Papers.aspx*

ISACA, *COBIT Focus* articles, *www.isaca.org/COBIT/focus/Pages/FocusHome.aspx*

Pressmann, Roger S.; *Software engineering: A practitioner's approac* h, McGraw Hill, USA, 2010

Singleton, Tommie W.; "Auditing Applications, Part 1," *ISACA Journal*, vol.

3, 2012, *https://www.isaca.org/Journal/archives/2012/Volume-3/Pages/Auditing-Applications-Part-1.aspx*

Singleton, Tommie W.; “Auditing Applications, Part 2,” *ISACA Journal*, vol. 4, 2012, *https://www.isaca.org/Journal/archives/2012/Volume-4/Pages/Auditing-Applications-Part-2.aspx*

Singleton, Tommie W.; “Auditing IT Risk Associated with Change Management and Application Development,” *ISACA Journal*, vol. 5, 2011, *https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/Auditing-IT-Risk-Associated-With-Change-Management-and-Application-Development.aspx*

Singleton, Tommie W.; “Testing Controls Associated With Data Transfers,” *ISACA Journal*, vol. 2, 2012, *https://www.isaca.org/Journal/archives/2012/Volume-2/Pages/Testing-Controls-Associated-With-Data-Transfers.aspx*

SELF-ASSESSMENT QUESTIONS

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often, a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided. Please note that these questions are not actual or retired exam items. Please see the section

“About This Manual” at the beginning of this manual for more guidance regarding practice questions.

To assist in testing an essential banking system being acquired, an organization has provided the vendor with sensitive data from its existing production system. An IS auditor's **PRIMARY** concern is that the data should be:

A. sanitized.

B. complete.

C. representative.

D. current.

3-2

Which of the following is the **PRIMARY** purpose for conducting parallel testing?

A. To determine whether the system is cost-effective

B. To enable comprehensive unit and system testing

C. To highlight errors in the program interfaces with files

D. To ensure the new system meets user requirements

3-3

When conducting a review of business process reengineering, an IS

auditor found that an important preventive control had been removed.

In this case, the IS auditor should:

A. inform management of the finding and determine whether

management is willing to accept the potential material risk of not having that preventive control.

B. determine if a detective control has replaced the preventive control during the process, and if it has not, report the removal of the preventive control.

C. recommend that this and all control procedures that existed before the process was reengineered be included in the new process.

D. develop a continuous audit approach to monitor the effects of the removal of the preventive control.

3-4

Which of the following data validation edits is effective in detecting transposition and transcription errors?

A. Range check

B. Check digit

C. Validity check

D. Duplicate check

3-5

Which of the following weaknesses would be considered the **MOST**

serious in enterprise resource planning software used by a financial organization?

A. Access controls have not been reviewed.

B. Limited documentation is available.

C. Two-year-old backup tapes have not been replaced.

D. Database backups are performed once a day.

3-6

When auditing the requirements phase of a software acquisition, an IS

auditor should:

A. assess the reasonability of the project timetable.

B. assess the vendor’s proposed quality processes.

C. ensure that the best software package is acquired.

D. review the completeness of the specifications.

3-7

An organization decides to purchase a software package instead of developing it. In such a case, the design and development phases of a traditional system development life cycle would be replaced with: A. selection and configuration phases

B. feasibility and requirements phases

C. implementation and testing phases

D. nothing, as replacement is not required.

3-8

User specifications for a software development project using the traditional (waterfall) system development life cycle methodology have not been met. An IS auditor looking for a cause should look in which of the following areas?

A. Quality assurance

B. Requirements

C. Development

D. User training

3-9

When introducing thin client architecture, which of the following types of risk regarding servers is significantly increased?

A. Integrity

B. Concurrency

C. Confidentiality

D. Availability

3-10 Which of the following procedures should be implemented to help ensure the completeness of inbound transactions via electronic data

interchange (EDI)?

A. Segment counts built into the transaction set trailer

B. A log of the number of messages received, periodically verified with the transaction originator

C. An electronic audit trail for accountability and tracking

D. Matching acknowledgment transactions received to the log of EDI messages sent

ANSWERS TO SELF-ASSESSMENT QUESTIONS

3-1

A.

Test data should be sanitized to prevent sensitive data from

leaking to unauthorized persons.

B.

Although it is important that the data set be complete, the

primary concern is that test data should be sanitized to prevent sensitive data from leaking to unauthorized persons.

C.

Although it is important to encompass a representation of the

transactional data, the primary concern is that test data should be sanitized to

prevent sensitive data from leaking to unauthorized persons.

D.

Although it is important that the data set represent current data being processed, the primary concern is that test data should be sanitized to prevent sensitive data from leaking to unauthorized persons.

3-2

A.

Parallel testing may show that the old system is more cost-

effective than the new system, but this is not the primary reason.

B.

Unit and system testing are completed before parallel testing.

C.

Program interfaces with files are tested for errors during system testing.

D.

The purpose of parallel testing is to ensure that the

implementation of a new system will meet user requirements.

3-3

A.

Those in management should be informed immediately to

determine whether they are willing to accept the potential

material risk of not having that preventive control in place.

B.

The existence of a detective control instead of a preventive control usually increases the risk that a material problem may occur.

C.

Often during business process reengineering, many nonvalue-added controls will be eliminated. This is good, unless they increase the business and financial risk.

D.

An IS auditor may wish to monitor or recommend that management monitor the new process, but this should be done only after management has been informed and accepts the risk of not having the preventive control in place.

3-4

A.

A range check is checking data that match a predetermined range of values.

B.

A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered (e.g., an incorrect, but valid, value substituted for the original). This control is

effective in detecting transposition and transcription errors.

C.

An availability check is programmed checking of the data validity in accordance with predetermined criteria.

D.

In a duplicate check, new or fresh transactions are matched to

those previously entered to ensure that they are not already in the system.

3-5

A.

A lack of review of access controls in a financial organization could have serious consequences given the types of data and

assets that could be accessed.

B.

A lack of documentation may not be as serious as not having

properly reviewed access controls.

C.

It may not even be possible to retrieve data from two-year-old

backup tapes.

D.

It may be acceptable to the business to perform database backups once a day, depending on the volume of transactions.

3-6

A.

A project timetable normally would not be found in a

requirements document.

B.

Assessing the vendor’s quality processes would come after the

requirements have been completed.

C.

The decision to purchase a package from a vendor would come

after the requirements have been completed.

D.

The purpose of the requirements phase is to specify the

functionality of the proposed system; therefore, an IS auditor would concentrate on the completeness of the specifications.

3-7

A.

With a purchased package, the design and development

phases of the traditional life cycle have become replaceable

with selection and configuration phases. A request for

proposal from the supplier of packaged systems is called for

and evaluated against predefined criteria for selection, before a decision is made to purchase the software. Thereafter, it is configured to meet the organization’s requirement.

B.

The other phases of the system development life cycle (SDLC)

such as feasibility study, requirements definition, implementation and post-implementation remain unaltered.

C.

The other phases of the SDLC such as feasibility study,

requirements definition, implementation and post-implementation

remain unaltered.

D.

In this scenario, the design and development phases of the

traditional life cycle have become replaceable with selection and configuration phases.

3-8

A.

Quality assurance has its focus on formal aspects of software

development such as adhering to coding standards or a specific

development methodology.

B.

To fail at user specifications implies that requirements

engineering has been done to describe the users’ demands.

Otherwise, there would not be a baseline of specifications to

check against.

C.

Obviously, project management has failed to either set up or

verify controls that provide for software or software modules under development that adhere to those specifications made

by the users.

D.

A failure to meet user specifications might show up during user

training or acceptance testing but is not the cause.

3-9

A.

Because the other elements do not need to change, the integrity

risk is not increased.

B.

Because the other elements do not need to change; the

concurrency risk is not increased.

C.

Because the other elements do not need to change, the

confidentiality risk is not increased.

D.

The main change when using thin client architecture is

making the servers critical to the operation; therefore, the

probability that one of them fails is increased and, as a result, the availability risk is increased.

3-10 **A.**

Control totals built into the trailer record of each segment is the only option that will ensure all individual transactions

sent are received completely.

B.

A log of the number of messages received provides supporting

evidence, but their findings are either incomplete or not timely.

C.

An electronic audit trail provides supporting evidence, but their findings are either incomplete or not timely.

D.

Matching acknowledgment transactions received to the log of

electronic data interchange (EDI) messages sent provides

supporting evidence, but their findings are either incomplete or not timely.

PART A: INFORMATION SYSTEMS

ACQUISITION AND DEVELOPMENT

3.0 INTRODUCTION

For an IS auditor to provide assurance that an organization's objectives are being met by the management practices of its information systems, it is important that the IS auditor understand how an organization evaluates, develops, implements, maintains and disposes of its information systems and related components.

Note: A CISA candidate should have a sound understanding of the information

systems (hardware and software) acquisition, development and implementation process. This understanding should extend beyond a definitional knowledge of terms and concepts and include an ability to identify vulnerabilities and risk and recommend appropriate controls to effectively mitigate risk. A thorough understanding of the phases of project management is also required. In addition, a CISA candidate should have a good understanding of various application systems and

architectures, and the related processes, risk and controls.

3.1 PROJECT GOVERNANCE AND MANAGEMENT

In any organization, several projects are typically running concurrently. In order to identify the relationships among those projects, a common approach is to establish a project portfolio and/or a program management structure.

This assists in identifying common objectives for the business organization, identifying and managing risk, and identifying resource connections.

All projects require governance structures, policies and procedures, and specific control mechanisms to assure strategic and tactical alignment with

the organization’s respective goals, objectives and risk management strategy.

Without proper governance, all aspects of a project may be compromised.

Project governance structures should involve the project and the functional line organization. All governance decisions about the project should be driven through the business case, and there must be periodic review of the benefits achieved.

Effective and efficient project management requires that projects be managed based on hard factors such as deliverables, quality, costs and deadlines; on soft factors such as team dynamics, conflict resolution, leadership issues, cultural differences and communication; and, finally, on environmental factors such as the political and power issues in the sponsoring organization, managing the expectations of stakeholders, and the larger ethical and social issues that may surround a project.

Project management structures are dependent on the size of the organization and

complexity of business/operations. Accordingly, some roles and responsibilities may be grouped or restructured.

Under such circumstances, the role of an IS auditor is to ensure that rules of system development, as they relate to segregation of duties (SoD) and responsibilities, are not compromised.

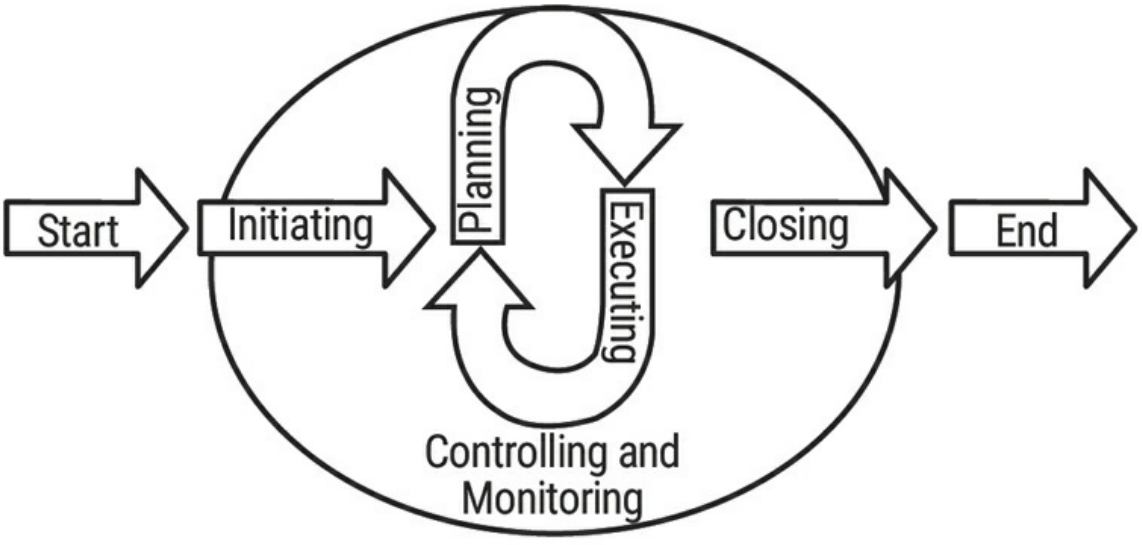
There are many approaches and standards to project management. Because there are significant differences in scope, content and wording in each of these approaches and standards, IS auditors must be familiar with the standard in use in their organization prior to involvement in specific projects.

Note: CISA candidates will not be tested on their knowledge of any particular project management approach or standard. However, they must understand the basic elements of project management structures, policies and procedures, and, more specifically, related controls.

3.1.1 PROJECT MANAGEMENT PRACTICES

Project management is the application of knowledge, skills, tools and

Figure 3.1—Project Management Life Cycle



techniques to a broad range of activities to achieve a stated objective such as meeting the defined user requirements, budget and deadlines for an IS

project. Project management is a business process in a project-oriented organization. The project management process begins with the project charter and ends with the completion of the project. Project management knowledge and practices are best described in terms of their component processes of initiating, planning, executing, controlling, monitoring and closing a project.

A typical project management process is depicted in **figure 3.1**.

Source: Adapted from *PMI, A Guide to the Project Management Body of Knowledge 5th Edition*, p. 50

The complexity of project management requires careful and explicit design of the project management process. Thus, all design issues applicable for business process engineering should be applied for the project management process.

3.1.2 PROJECT MANAGEMENT STRUCTURE

Three types of project management organizational structures outline the authority and control within an organization.

1. **Functional-structured organization**—In a functional-structured

organization, the project manager has only a staff function without formal management authority. The work is broken down in departments and a project manager is allowed to advise peers and team members only as to which activities should be completed.

2. **Project-structured organization**—In a project-structured organization, the project manager has formal authority over those taking part in the project. This includes authority over the project's budget, schedule and team.

3. **Matrix-structured project organization**—In a matrix-structured organization, management authority is shared between the project manager and the department heads.

IS projects may be initiated from within any part of the organization, including the IT department. An IS project has specific objectives, deliverables, and start and end dates. Most IS projects are divisible into explicit phases (e.g., SDLC).

Requests for major projects should be submitted to and prioritized by an IT

steering committee. The committee then identifies a project manager. The project manager, who need not be an IT staff member, should be given complete operational control over the project and be allocated the appropriate resources, including IS professionals and other staff from user departments, for the successful completion of the project. An IS auditor may be included in the project team as control expert. The IS auditor may also provide an independent, objective review to ensure that the level of involvement (commitment) of the responsible parties is appropriate. In such cases, the IS

auditor is not performing an audit but is participating on the project in an advisory role. Depending on the level of the IS auditor's involvement, he/she may become ineligible to perform audits of the application when it becomes operational. An example of a project's organizational structure is shown in

figure 3.2.

3.1.3 PROJECT MANAGEMENT ROLES AND RESPONSIBILITIES

The various roles and responsibilities of groups/individuals that may be

involved in the project management process follow:

• **Project steering committee**—Provides overall direction and ensures appropriate representation of the major stakeholders in the project's outcome. The project steering committee is ultimately responsible for all deliverables, project costs and schedules. This committee should be comprised of a senior representative from each business area that will be significantly impacted by the proposed new system or system modification.

The project manager should also be a member of this committee. Each member must have the authority to make decisions related to system designs that will affect their respective departments. Generally, a project sponsor assumes the overall ownership and accountability of the project and chairs the steering committee. The project steering committee performs the following functions:

– Reviews project progress regularly (e.g., semimonthly or monthly) and holds emergency meetings when required.

– Serves as coordinator and advisor. Members of the committee should be available to answer questions and make user-related decisions about system and program design.

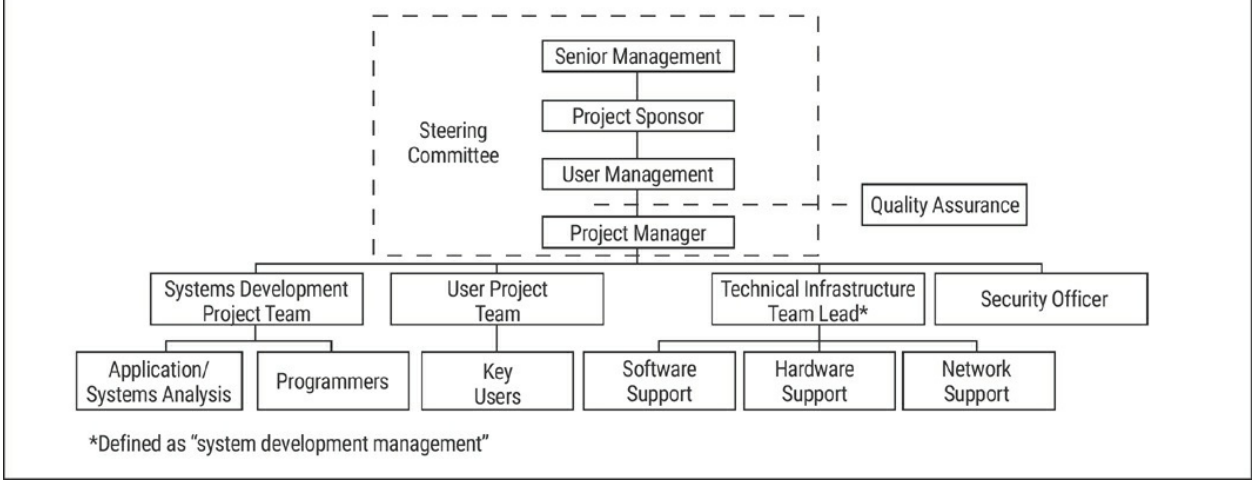
– Takes corrective action if necessary due to project progress and issues escalated to the committee.

• **Senior management**—Demonstrates commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

• **Project sponsor**—Provides funding for the project and works closely with the project manager to define the critical success factors (CSFs) and metrics for measuring the success of the project. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit the application will support.

• **User management**—Assumes ownership of the project and resulting system; allocates qualified representatives to the team; and actively participates in business process redesign, system requirements definition, test case development, acceptance testing and user training. User management should review and approve system deliverables as they are defined and implemented.

Figure 3.2—Project Management, Sample Organization Chart



• **User project team**—Completes assigned tasks, communicates effectively with the systems developers by actively involving themselves in the development process as subject matter experts (SMEs), works according to local standards

and advises the project manager of expected and actual project plan deviations

• **Project manager**—Provides day-to-day management and leadership of the project, ensures that project activities remain in line with the overall direction, ensures appropriate representation of the affected departments, ensures that the project adheres to local standards, ensures that deliverables meet the quality expectations of key stakeholders, resolves

interdepartmental conflicts, and monitors and controls costs and the project timetable. The project manager may facilitate the definition of the project scope, manage the budget and control the activities via a project schedule.

Where projects are staffed by personnel dedicated to the project, the project manager will have a line responsibility for such personnel.

• **Quality assurance (QA)**—Reviews results and deliverables within each phase and at the end of each phase and confirms compliance with

requirements. The objective of this group is to ensure the quality of the project by measuring the adherence of the project staff to the organization's SDLC, advise on deviations, and propose recommendations for process improvements or greater control points when deviations occur. The points where reviews occur depend on the SDLC methodology used, the structure and magnitude of the system and the impact of potential deviations.

Additionally, focus may include a review of appropriate, process-based activities related to either project management or the use of specific software engineering processes within a particular life cycle phase. Such a focus is crucial to completing a project on schedule and within budget and in achieving a given software process maturity level.

• **Systems development management**—Provides technical support for hardware and software environments by developing, installing and operating the requested system. This area also provides assurance that the system is compatible with the organization's computing environment and strategic IT direction and assumes operating support and maintenance activities after installation.

• **Systems development project team**—Completes assigned tasks, communicates effectively with users by actively involving them in the development process, works according to local standards and advises the project

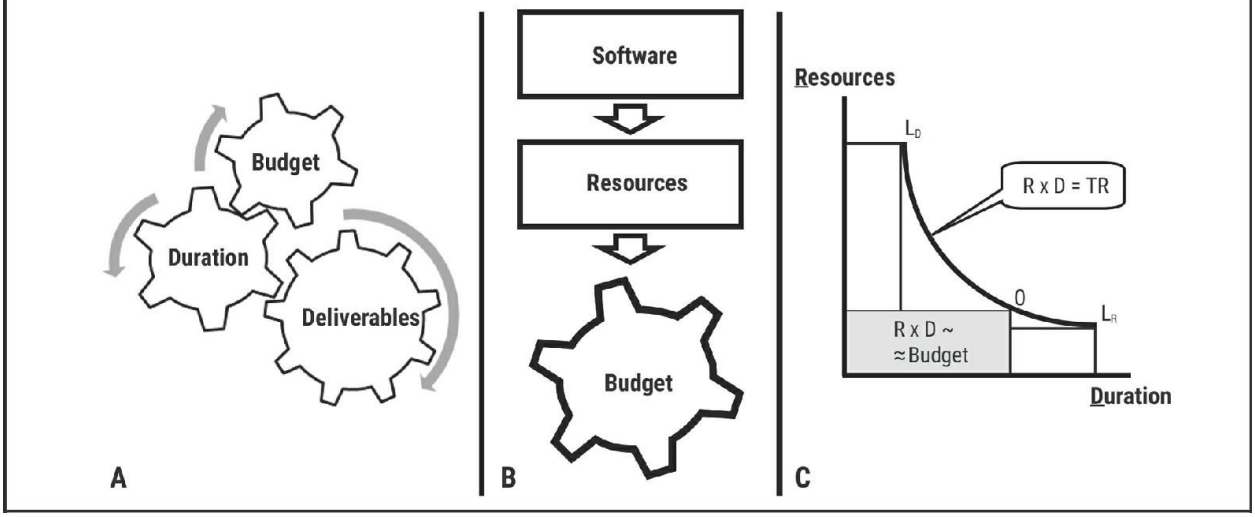
manager of necessary project plan deviations

• **Security officer (or security team)**—Ensures that system controls and supporting processes provide an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures; consults throughout the life cycle on appropriate security measures that should be incorporated into the system; reviews security test plans and reports prior to implementation; evaluates security-related documents developed in reporting the system's security effectiveness for accreditation; and periodically monitors the security system's effectiveness during its operational life

• **Information system security engineer**—Applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risk associated with these vulnerabilities. Key to meeting this role is defining the needs, requirements, architectures and designs to construct network, platform and application constructs according to the principles of both defense in breadth and security in depth.

Note: A CISA candidate should be familiar with the general roles and responsibilities of groups or individuals involved in the project management process.

Figure 3.3—Relationships Between Project Management Elements



3.1.4 PROJECT MANAGEMENT TECHNIQUES

A number of project management techniques and tools are available to assist the

project manager in controlling the time and resources utilized in the development of a system. The techniques and tools may vary from a simple manual effort to a more elaborate computerized process. The size and complexity of the project may require different approaches. Project management techniques also provide systematic quantitative and qualitative approaches to software size estimating, scheduling, allocating resources and measuring productivity. These tools and techniques typically aid in areas described in later sections in this chapter.

There are various elements of a project that should always be considered before selecting a technique. Their relationships are shown in **figure 3.3**.

Source: Personas & Técnicas Multimedia SL © 2009. All rights reserved. Used by permission.

Project management should pay attention to three key intertwining elements: deliverables, duration and budget (**figure 3.3A**). Their relationship is very complex but is shown in an oversimplified and schematized manner in the figure. Project duration and budget must be commensurate with the nature and characteristics of the deliverables. In general, there will be a positive correlation between highly demanding deliverables, a long duration and a high budget.

Budget is deduced **(figure 3.3B**) from the resources required to carry out the project by multiplying fees or costs by the amount of each resource.

Resources required by the project are estimated at the beginning of the project using techniques of software/project size estimation.

Size estimation yields a “total resources” calculation. Project management decides on the resources allocated at any particular moment in time. In general, it is convenient to assign an (almost) fixed amount of resources, thus probably minimizing costs (direct and administration). **Figure 3.3C** is simplified in its assumption that there is a fixed amount of resources during the entire project. The curve shows resources assigned (R) × duration (D) =

total resources (TR, a constant quantity); which is the classic “man × month”

dilemma curve. Any point along the curve meets the condition R × D = TR.

At any point O on the curve, the area of the rectangle will be TR, proportional to

the budget. If few resources are used, the project will take a long time (a point close to LR); if many resources are used, the project will take a shorter time (a point close to LD). LR and LD are two practical limits: a duration that is too long may not seem possible; use of too many (human) resources at once would be unmanageable.

3.1.5 PORTFOLIO/PROGRAM MANAGEMENT

A project portfolio is defined as all of the projects being carried out in an organization at a given point in time. A program is a group of projects and tasks that are closely linked together through common strategies, objectives, budgets and schedules. Portfolios, programs and projects are often controlled by a project management office (PMO), which governs the processes of project management but are not typically involved in the management of the content. Like projects, programs have a limited time frame (i.e., a defined start and end date) and organizational boundaries. A differentiator is that programs are more complex, usually have a longer duration, a higher budget and higher risk associated with them, and are of higher strategic importance.

A typical IS-related program may be the implementation of a large-scale enterprise resource planning (ERP) system that includes projects that address technology infrastructure, operations, organizational realignment, business

process reengineering (BPR) and optimization, training, and development.

Mergers and acquisitions (M&As) may serve as an example of a non–IS-related program that impacts both the gaining and/or divesting organizations'

IS architectures and systems, organizational structure, and business processes.

The objective of program management is the successful execution of programs including, but not limited to, the management of program:

• Scope, financials (costs, resources, cash flow, etc.), schedules, objectives and deliverables

• Context and environment

• Communication and culture

• Organization

To make autonomous projects possible while making use of synergies between related projects in the program, a specific program organization is required. Typical program roles are the:

• Program owner

• Program manager

• Program team

The program owner role is distinct from the project owner role. Typical communication structures in a program are program owner's meetings and program team's meetings. Methodology and processes used in program management are very similar to those in project management and run in parallel to each other. However, they must not be combined and have to be handled and carried out separately. To formally start a program, some form of written assignment from the program sponsor (owner) to the program manager and the program team is required. Because programs most often emerge from projects, such an assignment is of paramount importance to set the program context and boundaries as well as formal management authority.

In contrast to program management, in which all relevant projects are closely coupled, this is not a requirement in a project portfolio. Projects of a program belong to an organization's project portfolio as do projects that are not associated with a program.

To manage portfolios, programs and projects, an organization requires specific and well-designed structures such as expert pools, a PMO and project portfolio groups. Specific integrative tools such as project management guidelines, standard project plans and project management marketing instruments are also used.

3.1.6 PROJECT MANAGEMENT OFFICE

The PMO, as an owner of the project management and program management process, must be a permanent structure and adequately staffed to provide professional support in these areas to maintain current and develop new procedures and standards. The objective of the PMO is to improve project and

program management quality and secure project success, but it can focus only on activities and tasks and not on project or program content.

An IS auditor should be able to differentiate between auditing project content and/or procedural aspects of a program or project. The objectives of project portfolio management are:

• Optimization of the results of the project portfolio (not of the individual projects)

• Prioritizing and scheduling projects

• Resource coordination (internal and external)

• Knowledge transfer throughout the projects

Project Portfolio Database

A project portfolio database is mandatory for project portfolio management.

It must include project data such as owner, schedules, objectives, project type, status and cost. Project portfolio management requires specific project portfolio reports. Typical project portfolio reports are a project portfolio bar chart, a profit versus risk matrix and a project portfolio progress graph.

Example:

A. An organization is migrating from legacy applications to an ERP

system and has the strategic goal of delivering cutting-edge computers and maintaining high cash flow to continue to fund research and

development. To do so, the organization is using its:

1. Internal pool of application developers to code its strategic business

process of the manufacture of newly designed computers to deliver finished goods and sales order to cash receipts considering the

sensitivity of its business model.

2. Vendors to code the nonstrategic business processes of procure to pay and financial accounting.

B. The organization is also pursuing a program for outsourcing

transactional processes to a third-party service provider for online sales and a payment portal.

In this context, activities A.1, A.2 and B, individually, are projects. Activities A.1 and A.2 represent a single program, as they are part of the single larger activity of migrating from legacy applications to ERP, and activity B is part of another larger program to outsource noncore manufacturing processes.

Activities A.1, A.2 and B (assuming these are the only activities underway in the entity) represent the portfolio for the entity.

3.1.7 PROJECT BENEFITS REALIZATION

The objective of benefits realization is to ensure that IT and the business fulfill their value management responsibilities, particularly that:

• IT-enabled business investments achieve the promised benefits and deliver measurable business value.

• Required capabilities (solutions and services) are delivered:

– On time, both with respect to schedule and time-sensitive market, industry and regulatory requirements

– Within budget

• IT services and other IT assets continue to contribute to business value.

See chapter 2, Governance and Management of IT, for more details on benefits realization.

For projects, a planned approach to benefits realization is required, looking beyond project cycles to longer-term cycles that consider the total business benefits and total business costs throughout the life of the new system.

Benefits rarely come about exactly as envisioned in plans. An organization has to keep checking and adjusting strategies. Key elements of project

benefits realization are:

• Describing benefits management or benefits realization

• Assigning a measure and target

• Establishing a tracking/measuring regimen

• Documenting the assumption

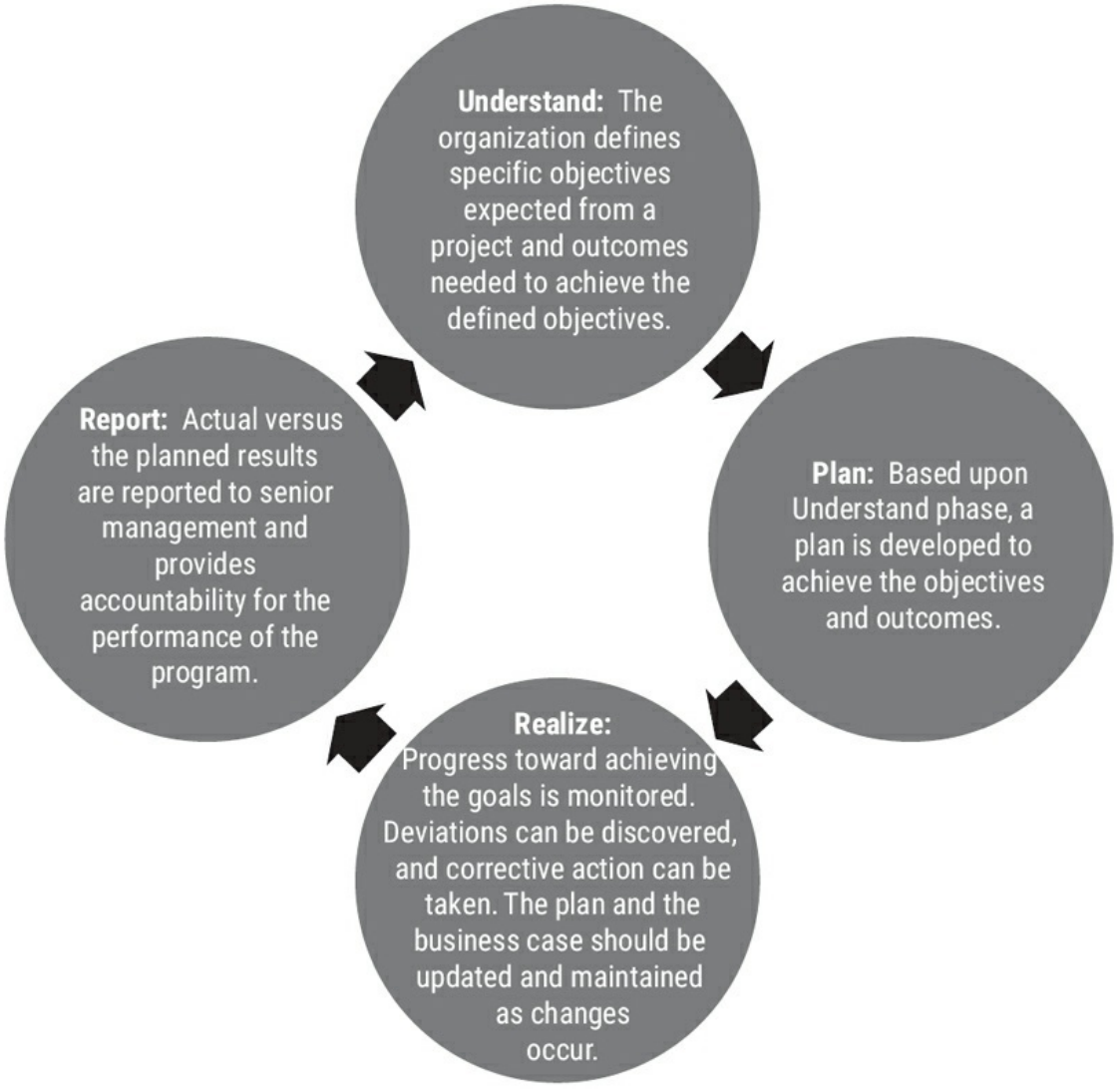
• Establishing key responsibilities for realization

• Validating the benefits predicted in the business

• Planning the benefit that is to be realized

Generally, benefits realization at the project level encompasses four phases, as indicated in the **figure 3.4**.

Figure 3.4—Benefits Realization Phases—Project Level



Source: New South Wales Government Department of Finance & Services, *Benefits Realisation Guideline, Version 1.2*, Australia, 2011

Project benefits realization is a compromise among major factors such as cost, quality, development/delivery time, reliability and dependability.

Strategy-makers perform a comprehensive study and evaluate which factors are "qualifying" or "winning" and then compare those factors with strengths, weaknesses and competencies of services available to complete and maintain systems. Most large organizations employ structured project management

principles to support changes to their information systems environment.

As a starting point, an IS auditor should understand how the business defines value or a return on investment (ROI) for development-related projects. If an organizations fails to consistently meet its ROI objectives, this may suggest weakness in its SDLC and related project management practices.

Example:

An organization is planning to invest in an application that would enable customers to manager their orders online. The following would be relevant for the ROI calculation:

A. Business costs

1. Cost of developing the online application

2. Cost of controls to ensure integrity of data at rest and in process, while ensuring nonrepudiation

B. Business benefits

1. Increase in operating profits attributable to expected spike in business driven by customer satisfaction (percent of revenue)

2. Reduction in operating costs (in terms of dedicated personnel who previously interacted with customers and executed changes)

ROI may be measured as value of benefit/costs, which then can be compared with an organization's cost of funds, to make a go/no-go decision. This ROI framework can then be used as a benchmark to evaluate the progress of the project and identify causes, if the actual ROI is not aligning with the planned ROI.

Project benefits realization is a continuous process that must be managed just like any business process. Assessment of the benefits realization processes and the business case should be a key element of benefits realization processes. Benefits realization often includes a post-implementation review after the implementation of systems. Time must be allowed for initial technical problems to be resolved and for the project benefits to accrue as users become familiar

with the new processes and procedures. Project benefits realization must be part of the governance and management of a project and include business sponsorship.

3.1.8 PROJECT INITIATION

A project is initiated by a project manager or sponsor gathering the information required to gain approval for the project to be created. This is often compiled into terms of reference or a project charter that states the objective of the project, the stakeholders in the system to be produced, and the project manager and sponsor. Approval of a project initiation document (PID) or a project request document (PRD) is the authorization for a project to begin. Depending on the size and complexity of the project and the affected parties, the initiation of a project may be achieved by:

• **One-on-one meetings**—One-on-one meetings and a project start workshop help to facilitate two-way communication between the project team members and the project manager.

• **Kick-off meetings**—A kick-off meeting may be used by a project manager to inform the team of what has to be done for the project. Communications involving significant project events should be documented as part of the project artifacts (i.e., project charter meeting, kick-off meeting, gate reviews, stakeholder meetings, etc.).

• **Project start workshops**—A preferred method to ensure that communication is open and clear among the project team members is to use a project start workshop to obtain cooperation from all team members and buy-in from stakeholders. This helps develop a common overview of the project and communicates the project culture early in the project.

• **A combination of the three**—An organization may choose to use two or more of these methods to initiate a project.

3.1.9 PROJECT OBJECTIVES

Project objectives are the specific action statements that support attainment of project goals. All project goals will have one or more objectives identified as the actions needed to reach that goal. The project objective is the means to meet the project goal.

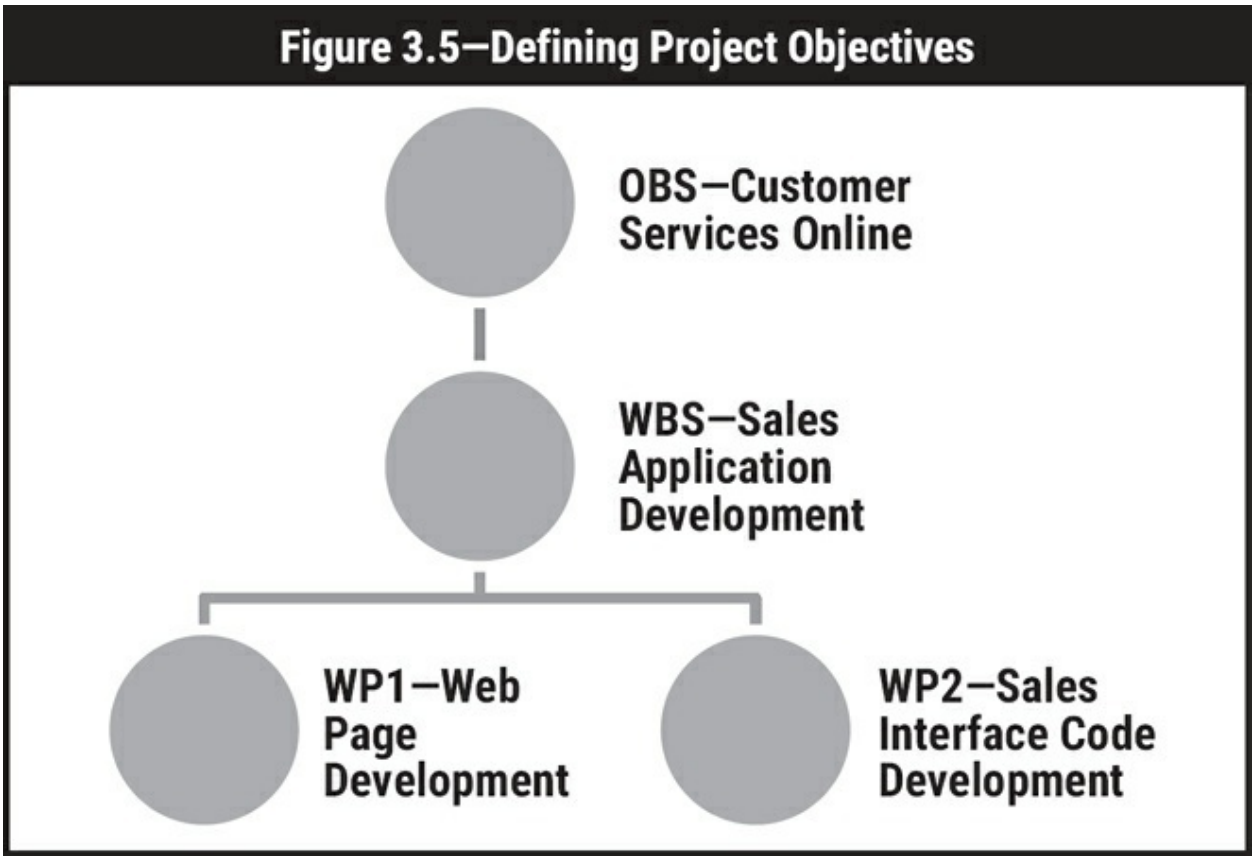
A project must have clearly defined results that are specific, measurable, attainable, realistic and timely (SMART). A commonly accepted approach to define project objectives is to start off with an object breakdown structure (OBS). It represents the individual components of the solution and their

relationships to each other in a hierarchical manner, either graphically or in a table. An OBS can help, especially when dealing with intangible project results such as organizational development, to ensure that a material deliverable is not overlooked.

After the OBS has been compiled or a solution is defined, a work breakdown structure (WBS) is designed to structure all the tasks that are necessary to build up the elements of the OBS during the project. The WBS represents the project in terms of manageable and controllable units of work, serves as a central communications tool in the project, and forms the baseline for cost and resource planning.

In contrast to the OBS, the WBS does not include basic elements of the solution to build but shows individual work packages (WPs) instead. The structuring of the WBS is process-oriented and in phases. The level of detail of the WBS serves as the basis for the negotiations of detailed objectives among the project sponsor, project manager and project team members.

Figure 3.5 shows an example of this process.



Detailed specifications regarding the WBS can be found in WPs. Each WP

must have a distinct owner and a list of main objectives and may have a list of additional objectives and out-of-scope objectives. The WP specifications should include dependencies on other WPs and a definition of how to evaluate performance and goal achievement. An example of a WBS is shown in **figure 3.6**.

Key things to remember with WBS and respective WPs include the

following:

• The top WBS level represents the final deliverable or project.

• Subdeliverables contain WPs that are assigned to an organization’s department or unit.

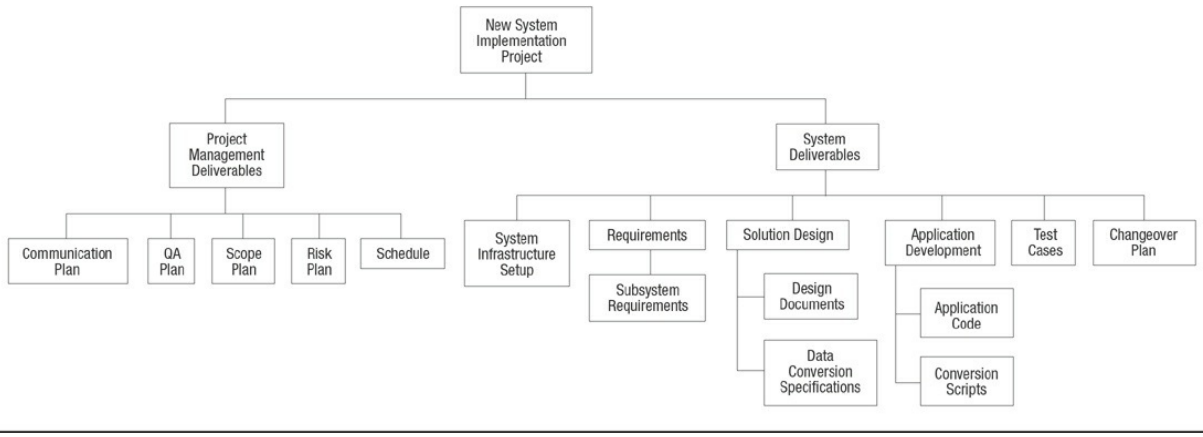
• All elements of the WBS do not need to be defined to the same level.

• WPs define the work, duration and costs for the tasks required to produce the subdeliverable.

• WPs should not exceed a duration of 10 days.

• WPs need to be independent of each other in the WBS.

Figure 3.6—Sample Work Breakdown Structure



• WPs are unique and should not be duplicated across the WBS.

To support communications, task lists are often used. A task list is a list of actions to be carried out in relation to WPs and includes assigned responsibilities and deadlines. The task list aids the individual project team members in operational planning and in making agreements. These task lists are most typically compiled into a project schedule at the planning phase of a project and are used in the controlling phase of the project to monitor and track the progress and completion of the WPs. Project schedules are living documents and should indicate the tasks for a WP, the start and finish dates, percentage completed, task dependencies and resource names of individuals planned to work on those tasks. A project schedule will also indicate the stage boundaries explained in section 3.2, Business Case and Feasibility Analysis.

3.1.10 PROJECT PLANNING

A project must be planned and controlled. A project manager should determine the following:

• Scope of the project (with agreement from stakeholders on project scope)

• Various tasks that need to be performed to produce the expected business application system

• Sequence or order in which these tasks need to be performed

• Duration or the time window for each task

• Priority of each task

• IT and non-IT supporting resources that are available and required to perform these tasks

• Budget or costing for each of these tasks

• Source and means of funding for labor, services, materials, and plant and equipment resources involved in the project

Several different sizing and measurement techniques are used and described in the sections that follow.

Information System Development Project Cost Estimation

Normally relatively large in scope and size, an information system development project focuses on a more complete and integrated solution (hardware, software, facilities, services, etc.) Therefore, these types of projects require much greater planning with regard to estimating and budgeting.

Four commonly used methodologies to estimate the cost of an information system acquisition and development project are:

• **Analogous estimating**—By using estimates from prior projects, the project manager can develop the estimated cost for a new project. This is the quickest estimation technique.

• **Parametric estimating**—The project manager looks at the same past data that were used in analogous estimating and leverages statistical data (estimated employee hours, materials costs, technology, etc.) to develop the estimate. This approach is more accurate than analogous estimation.

• **Bottom-up estimating**—In this method, the cost of each activity in the project

is estimated to the greatest detail (i.e., starting at the bottom), and then all the costs are added to arrive at the cost estimate of the entire project. While the most accurate estimate, this is the most time-consuming approach.

• **Actual costs**—Like analogous estimation, this approach takes an extrapolation from the actual costs that were incurred on the same system during past projects.

Software Size Estimation

Software size estimation relates to methods of determining the relative

physical size of the application software to be developed. Estimates can be used to guide the allocation of resources, judge the time and cost required for its development, and compare the total effort required by the resources.

Traditionally, software sizing has been performed using single-point estimations (based on a single parameter) such as source lines of code (SLOC). For complex systems, single-point estimation techniques have not worked because they do not support more than one parameter in different types of programs, which, in turn, affects the cost, schedule and quality metrics. To overcome this limitation, multiple-point estimations have been designed.

Current technologies now take the form of more abstract representations such as diagrams, objects, spreadsheet cells, database queries and graphical user interface (GUI) widgets. These technologies are more closely related to

“functionality” deliverables rather than “work” or lines that need to be created.

Function Point Analysis

The function point analysis (FPA) technique is a multiple-point technique used for estimating complexity in developing large business applications.

The results of FPA are a measure of the size of an information system based on the number and complexity of the inputs, outputs, files, interfaces and queries with which a user sees and interacts. This is an indirect measure of software size and the process by which it is developed versus direct size-oriented measures such as SLOC counts.

Function points (FPs) are computed by first completing a table **(figure 3.7**) to

determine whether a particular entry is simple, average or complex. Five FP

count values are defined, including the number of user inputs, user outputs, user inquiries, files and external interfaces.

Upon completion of the table entries, the count total in deriving the function point is computed through an algorithm that considers complexity adjustment values (i.e., rating factors) based on responses to questions related to issues

such as reliability, criticality, complexity, reusability, changeability and portability. Function points derived from this equation are then used in a manner analogous to SLOC counts as a measure for cost, schedule, productivity and quality metrics (e.g., productivity = FP/person-month, quality = defects/FP, and cost = $/FP).

FPA is an indirect measurement of the software size.

Note: The CISA candidate should be familiar with the use of FPA; however, the CISA exam does not test the specifics on how to perform an FPA calculation.

FPA behaves reasonably well in estimating business applications but not as well for other types of software (such as OS, process control,

communications and engineering). Other estimation methods are more appropriate for such software and include the constructive cost model (COCOMO) and FPA feature points of De Marco and Watson-Felix.

Cost Budgets

A system development project should be analyzed with a view to estimating the amount of effort that will be required to carry out each task. The estimates for each task should contain some or all of the following elements:

• Personnel hours by type (e.g., system analyst, programmer, clerical)

• Machine hours (predominantly computer time as well as duplication facilities, office equipment and communication equipment)

• Other external costs such as third-party software, licensing of tools for the project, consultant or contractor fees, training costs, certification costs (if

required), and occupation costs (if extra space is required for the project) Having established a best estimate of expected work efforts by task (i.e., actual hours, minimum/maximum) for personnel, costs budgeting now becomes a two-step process to achieve the following results:

1. Obtain a phase-by-phase estimate of human and machine effort by summing the expected effort for the tasks within each phase.

2. Multiply the effort expressed in hours by the appropriate hourly rate to

Figure 3.7—Computing Function Point Metrics

Measurement Parameter	Count	Weighting Factor			
		Simple	Average	Complex	Results
Number of user inputs		× 3	4	6	=_____
Number of user outputs		× 4	5	7	=_____
Number of user inquiries		× 3	4	6	=_____
Number of files		× 7	10	15	=_____
Number of external interfaces		× 5	7	10	=_____
Count total:					

obtain a phase-by-phase estimate of systems development expenditure.

Other costs may require tenders or quotes.

Software Cost Estimation

Cost estimation is a result of software size estimation and helps to properly scope a project. Automated techniques for cost estimation of projects at each phase of information system development are available. To use these products, an information system is usually divided into main components and a set of cost drivers is established. Components include:

• Source code language

• Execution time constraints

• Main storage constraints

• Data storage constraints

• Computer access

• The target machine used for development

• The security environment

• Staff experience

After all the drivers are defined, the program will develop cost estimates of the information system and total project.

Scheduling and Establishing the Time Frame

While budgeting involves totaling the human and machine effort involved in each task, scheduling involves establishing the sequential relationship among tasks. This is achieved by arranging tasks according to the following two elements:

Note: Organizations that use FP methods develop criteria for determining whether a particular entry is simple, average or complex.

• Earliest start date, by considering the logical sequential relationship among tasks and attempting to perform tasks in parallel, wherever possible

• Latest expected finish date, by considering the estimate of hours per the budget and the expected availability of personnel or other resources, and allowing for known, elapsed-time considerations (e.g., holidays, recruitment time, full-time/part-time employees)

The schedule can be graphically represented using various techniques such as Gantt charts, the critical path method (CPM) or program evaluation and review technique (PERT) diagrams. During the project execution, the budget and schedule should be revisited to verify compliance and identify variances at key points and milestones. Any variances to the budget and schedule should be analyzed to determine the cause and corrective action to take in minimizing or eliminating the total project variance. Variances and the variance analysis should be reported to management on a timely basis.

Gantt Charts

Gantt charts **(figure 3.8)** aid in scheduling the activities (tasks) needed to complete a project. The charts show when an activity should begin and when it

should end along a timeline. The charts also show which activities can occur concurrently and which must be completed sequentially. Gantt charts can also reflect the resources assigned to each task and by what percent allocation, as well as aiding in identifying activities that have been completed early or late by comparison to a baseline. Progress of the entire project can be ascertained to determine whether the project is behind, ahead or on schedule compared to the baseline project plan. Gantt charts can also be used to track the achievement of milestones or significant accomplishments for the project such as the end of a project phase or completion of a key deliverable.

Critical Path Methodology

The critical path is the sequence of activities that produces the longest path through a project. All project schedules have (at least) one critical path, usually only one in nonmanipulated project schedules. Critical paths are important because, if everything goes according to schedule, they help estimate the shortest possible completion time for the overall project.

Activities that are not in the critical path have slack time, which is the difference between the latest possible completion time of each activity that will not delay the completion of the overall project and the earliest possible completion time based on all predecessor activities. Activities on a critical path have zero slack time. By working through the network forwards and backwards, the earliest possible completion time for the activities and the project are determined.

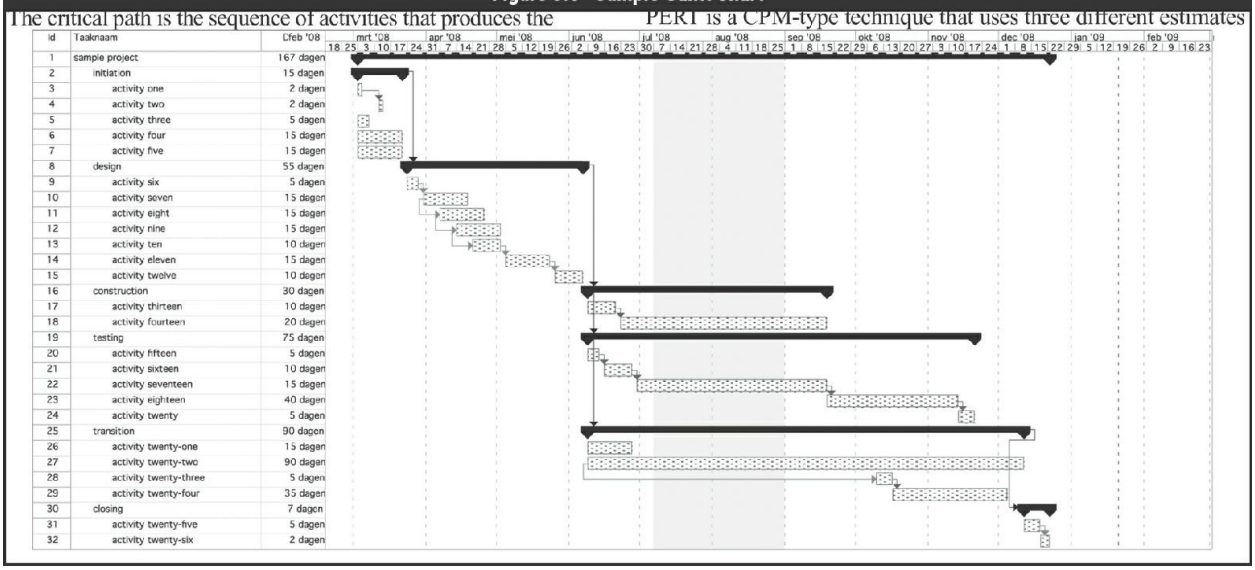
All project schedules have a critical path. Because the activities of a project are ordered and independent, a project can be represented as a network in which activities are shown as branches connected at nodes immediately preceding and immediately following activities. A path through the network is any set of successive activities that go from the beginning to the end of the project. Associated with each activity in the network is a single number that best estimates the amount of time the activity will consume.

Most CPM packages facilitate the analysis of resource utilization per time unit (e.g., day, week) and resource leveling, which is a way to level off resource peaks and valleys. Resource peaks and valleys are expensive due to management, hiring, firing, and/or overtime and idle resource costs. A constant, base resource utilization is preferable. There are few, if any, scientific (algorithmic) resource-leveling methods available, but there is a battery (which

CPM packages offer) of efficient heuristic methods that yield satisfactory results.

Figure 3.8—Sample Gantt Chart

The critical path is the sequence of activities that produces the PERT is a CPM-type technique that uses three different estimates



id	Taaknaam	Dfeb '08
1	sample project	167 dagen
2	initiation	15 dagen
3	activity one	2 dagen
4	activity two	2 dagen
5	activity three	5 dagen
6	activity four	15 dagen
7	activity five	15 dagen
8	design	55 dagen
9	activity six	5 dagen
10	activity seven	15 dagen
11	activity eight	15 dagen
12	activity nine	15 dagen
13	activity ten	10 dagen
14	activity eleven	15 dagen
15	activity twelve	10 dagen
16	construction	30 dagen
17	activity thirteen	10 dagen
18	activity fourteen	20 dagen
19	testing	75 dagen
20	activity fifteen	5 dagen
21	activity sixteen	10 dagen
22	activity seventeen	15 dagen
23	activity eighteen	40 dagen
24	activity twenty	5 dagen
25	transition	90 dagen
26	activity twenty-one	15 dagen
27	activity twenty-two	90 dagen
28	activity twenty-three	5 dagen
29	activity twenty-four	35 dagen
30	closing	7 dagen
31	activity twenty-five	5 dagen
32	activity twenty-six	2 dagen

Program Evaluation Review Technique

PERT is a CPM-type technique that uses three different estimates of each activity duration. The three estimates are reduced to a single number (by applying a mathematical formula), and then the classic CPM algorithm is applied. PERT is often used in system development projects with uncertainty about the duration (e.g., pharmaceutical research or complex software development). A diagram illustrating the use of the PERT network management technique is shown in **figure 3.9**, in which events are points in time or milestones for starting and completing activities (arrows). To determine a task's completion, three estimates are shown for completing each activity. The first is the best-case (optimistic) scenario and the third is the worst-case (pessimistic) scenario. The second is the most likely scenario.

This estimate is based on experience attained from projects similar in size and scope. To calculate the PERT time estimate for each given activity, the following calculation is applied:

[Optimistic + Pessimistic + 4(most likely)]/6

Using PERT, a critical path is also derived. The critical path is the longest path through the network (only one critical path in a network). The critical path is the route along which the project can be shortened (accelerated) or lengthened

(delayed). In **figure 3.9**, the critical path is A, C, E, F, H and I.

The advantage of PERT over CPM in the example provided is that the formula is based on the reasonable assumption that the three time estimates follow a beta statistical distribution and, accordingly, probabilities (with associated confidence levels) can be associated with the total project duration.

When designing a PERT network for system development projects, the first step is to identify all the activities and related events/milestones of the project and their relative sequence. For example, an event or result may be the completion of the operational feasibility study or the point at which the user accepts the detailed design. The analyst must be careful not to overlook any activity. Additionally, some activities such as analysis and design must be preceded by others before program coding can begin. The list of activities determines the detail of the PERT network. The analyst may prepare many diagrams that provide increasingly detailed time estimates.

Timebox Management

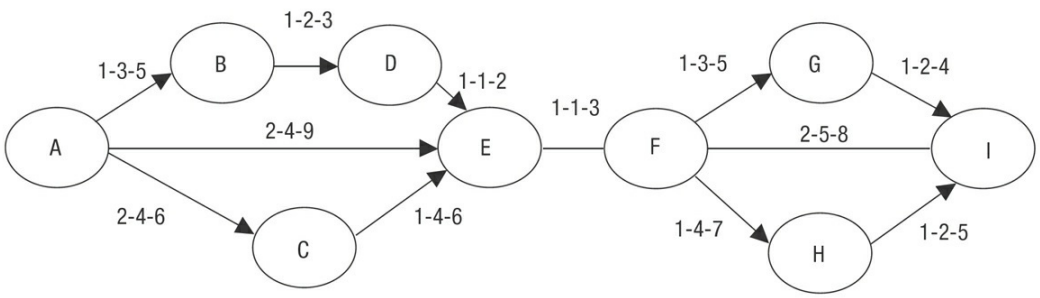
Timebox management is a project management technique for defining and deploying software deliverables within a relatively short and fixed period of time and with predetermined specific resources. There is a need to balance software quality and meet the delivery requirements within the timebox.

Timebox management can be used to accomplish prototyping or rapid application development-type approaches in which key features are to be delivered in a short time frame. Key features include interfaces for future integrations. The major advantage of this approach is that it prevents project cost overruns and delays from scheduled delivery. The project does not necessarily eliminate the need for a quality process. The design and development phase is shortened due to the use of newer developmental tools and techniques. Preparation of test cases and testing requirements are easily written down as a result of end-user participation. System test and user acceptance testing (UAT) are normally performed together.

3.1.11 PROJECT EXECUTION

Once planning efforts have been completed, the program manager, in coordination with the PMO, starts the actual project execution of the planned tasks as described in the plans, processes and procedures. The program and

Figure 3.9—PERT Network-based Chart



project management team initiates monitoring of internal team production and quality metrics and monitors these metrics from contractors and vendors.

A key success factor is the project's oversight of the integrated team in the IT

system requirements, architecture, design, development, testing, implementation and transitioning to production operations.

3.1.12 PROJECT CONTROLLING AND MONITORING

The controlling and monitoring activities of a project include management of scope, resource usage and risk. It is important that new requirements for the project be documented and, if approved, allocated appropriate resources.

Control of change during a project ensures that projects are completed within stakeholder requirements of time, use of funds and quality objectives.

Stakeholder satisfaction should be addressed with effective and accurate requirements capture, proper documentation, baselining and skilled steering committee activity.

To monitor and measure the development effort, metrics are required. The first step is to identify resources (e.g., people with requisite skills, development tools, facilities) for information system and software development. This will help in estimating and budgeting system and software development resources.

Management of Scope Changes

Managing the scope of projects requires careful documentation in the form of a WBS. This documentation forms part of the project plan or the project baseline.

Changes to the scope almost invariably lead to changes in required

activities and impact deadlines and budget. Therefore, it is necessary to have a change management process, including a formal change request submitted to the project manager. Only stakeholders are allowed to submit change requests. Copies of all change requests should be archived in the project file.

The project manager judges the impact of each change request on project activities (scope), schedule and budget. The change advisory board then evaluates the change request (on behalf of the sponsor) and decides whether to recommend the change. If the change is accepted, the project manager is instructed to update the project plan to reflect the requested change. The updated project plan must be formally confirmed by the project sponsor—

accepting or rejecting the recommendation of the change advisory board.

Management of Resource Usage

Resource usage is the process by which the project budget is being spent. To determine whether actual spending is in line with planned spending, resource usage must be measured and reported. In addition to spending, productivity must be monitored to determine if resource allocation is on task. Whether this is actually happening can be checked with a technique called earned value analysis (EVA).

EVA consists of comparing the metrics at regular intervals during the project such as:

• Budget to date

• Actual spending to date

• Estimate to complete

• Estimate at completion

For example, if a single-task project is planned to take three working days, with eight hours spent each day, the resource will have spent eight hours after the first day, with 16 hours remaining. In order to know if the project is on track, the employee should be asked how much additional time is required to complete the

task. If the answer exceeds 16, the project is overrun and not on track.

Management of Risk

Risk is defined as an uncertain event or condition that would impact relevant

aspects of the project. There are two main categories of project risk: the category that impacts the business benefits (and, therefore, endangers the reasons for the project's very existence) and the category that impacts the project itself. The project sponsor is responsible for mitigating the first category of risk and the project manager is responsible for mitigating the second category.

See chapter 2, Governance and Management of IT, for more information.

3.1.13 PROJECT CLOSING

A project has a finite life so, at some point, it must be closed, and a new or modified system is handed over to the users and/or system support staff. At this point, any outstanding issues will need to be assigned. The project sponsor should be satisfied that the system produced is acceptable and ready for delivery.

Key questions to consider include:

• When will the project manager issue the final project closure notification?

• Who will issue the final project notification?

• How will the project manager assist the project team transition to new projects or release them to their regular assigned duties?

• What will the project manager do for actions, risk and issues that remain open? Who will pick up these actions and how will these be funded?

Hand-off of relevant documentation and duties will occur at this stage, and the project team and other relevant stakeholders will identify lessons learned from the project.

Review may be a formal process such as a post-project review. A postimplementation review, in contrast, is typically completed after the project has been in use (or in "production") for some time—long enough to realize its

business benefits and costs and measure the project's overall success and impact on the business units. Metrics used to quantify the value of the project include total cost of ownership (TCO) and ROI.

3.1.14 IS AUDITOR'S ROLE IN PROJECT MANAGEMENT

To achieve a successful project outcome, the audit function should play an active role, where appropriate, in the life cycle development of a new system or business application. This will facilitate efforts to ensure that proper controls are designed and implemented in the new system (e.g., continuous concurrent controls for paperless ecommerce systems). An IS auditor needs to understand the system or application being developed in order to identify potential vulnerabilities and points requiring control. If controls are lacking or the process is disorderly, it is an IS auditor's role to advise the project team and senior management of the deficiencies. It may also be necessary to advise those engaged in information systems acquisition and development activities of appropriate controls or processes to implement and follow.

An IS auditor's role may take place during the project or upon completion.

Tasks generally include the following:

• Meet with key systems development and user project team members to determine the main components, objectives and user requirements of the system to identify the areas that require controls.

• Discuss the selection of appropriate controls with systems development and user project team members to determine and rank the major risk to and exposures of the system.

• Discuss references to authoritative sources with systems development and user project team members to identify controls to mitigate the risk to and exposures of the system.

• Evaluate available controls and participate in discussions with systems development and user project team members to advise the project team regarding the design of the system and implementation of controls.

• Periodically meet with systems development and user project team members and review the documentation and deliverables to monitor the systems

development process to ensure that controls are implemented, user and business requirements are met, and the systems

development/acquisition methodology is being followed. Review and evaluate application system audit trails to ensure that documented controls are in place to address all security, edit and processing controls. Tracking information in a change management system includes:

– History of all work order activity (date of work order, programmer assigned, changes made and date closed)

– History of logons and logoffs by programmers

– History of program deletions

– Adequacy of SoD and QA activities

• Identify and test existing controls to determine the adequacy of production library security to ensure the integrity of the production resources.

• Review and analyze test plans to determine if defined system requirements are being verified.

• Analyze test results and other audit evidence to evaluate the system maintenance process to determine whether control objectives were achieved.

• Review appropriate documentation, discuss with key personnel and use observation to evaluate system maintenance standards and procedures to ensure their adequacy.

• Discuss and examine supporting records to test system maintenance procedures to ensure that they are being applied as described in the standards.

• Participate in post-implementation reviews.

3.2 BUSINESS CASE AND FEASIBILITY ANALYSIS

A business case provides the information required for an organization to decide whether a project should proceed. Depending on the organization and the size of the investment, the development of a business case is either the first step in a

project or a precursor to the start of a project. A business case should adequately describe the business reasons or benefits for a project and be of sufficient detail to describe the justification for initiating and continuing a project. It should answer the question, “Why should this project be undertaken and/or continued?” A business case should be a key element of the decision process throughout the life cycle of any project. If at any stage the business case is thought to no longer be valid, the project sponsor or IT

steering committee should consider whether the project should proceed. In a well-planned project, there will be decision points, often called “stage gates”

or “kill points,” at which a business case is formally reviewed to ensure that it is still valid. If the business case changes during the course of an IT project, the project should be reapproved through the departmental planning and approval process.

After the initial approval has been given to move forward with a project, an analysis begins to clearly define the need and identify alternatives for addressing the need. This analysis is known as the feasibility study. An initial business case would normally derive from a feasibility study undertaken as part of project initiation/planning. This is an early study of a problem to assess if a solution is practical and meets requirements within established budgets and schedule requirements. A feasibility study will normally include the following six elements:

1. **Project scope**—Definition of the business problem and/or opportunity to be addressed. It should be clear, concise and to the point.

2. **Current analysis**—Definition and establishment of an understanding of a system, a software product, etc. Based on this analysis, it may be determined that the current system or software product is working correctly, some minor modifications are needed, or a complete upgrade or replacement is required. At this point in the process, the strengths and weaknesses of the current system or software product are identified.

3. **Requirements**—Definition of project requirements based upon stakeholder needs and constraints. Defining requirements for software differs from defining requirements for systems. The following are examples of needs and constraints used to define requirements:

• Business, contractual and regulatory processes

• End-user functional needs

• Technical and physical attributes defining operational and engineering parameters

4. **Approach**—Definition of a course of action to satisfy the requirements for a recommended system and/or software solution. This step clearly identifies the alternatives that were considered and the rationale as to why the preferred solution was selected. This is the process wherein the use of existing structures and commercial alternatives are considered (e.g., “build versus buy” decisions).

5. **Evaluation**—Examination of the cost-effectiveness of the project based upon the previously completed elements within the feasibility study. The final report addresses the cost-effectiveness of the approach selected.

Elements of the final report include:

• The estimated total cost of the project if the preferred solution is selected, along with the alternates to provide a cost comparison,

including:

– Estimate of employee hours required to complete

– Material and facility costs

– Vendors and third-party contractors’ costs

– Project schedule start and end dates

• A cost and evaluation summary encompassing cost-benefit analysis, ROI, etc.

6. **Review**—Reviews (formal) of the previously completed elements of the feasibility study to both validate the completeness and accuracy of the feasibility study and render a decision to either approve or reject the project or ask for corrections before making a final decision. The review and report are conducted with all key stakeholders. If the feasibility study is approved, all key stakeholders sign the document. Rationale for rejection of the feasibility study

should be explained and attached to the document as part of a lesson-learned list for use in future project studies.

3.2.1 IS AUDITOR'S ROLE IN BUSINESS CASE DEVELOPMENT

An IS auditor should understand how a business defines business cases used during feasibility studies and resultant determinations with regard to ROI for information systems development-related projects. If an organization fails to consistently meet its ROI objectives, this may suggest weaknesses in its system development approach and related project management practices.

An IS auditor plays an important role in the review and evaluation of a feasibility study. This is to ensure that the process and decisions were made in an effective and unbiased manner. The following are tasks typically performed by an IS auditor when reviewing a feasibility study:

• Review and evaluate the criticality of the business and information system process requirements.

• Determine if a solution can be achieved with systems already in place. If not, review the evaluation of alternative solutions for reasonableness.

• Determine the reasonableness of the chosen solution based on their strengths and weaknesses.

• Determine whether all cost justifications/benefits are verifiable and reflect

anticipated costs and benefits to be realized.

• Review the documentation produced for reasonableness.

As it applies to the requirements definition within a feasibility study, an IS

auditor should perform the following functions:

• Obtain the detailed requirements definition document and verify its accuracy and completeness through interviews with the relevant user departments.

• Identify the key team members on the project team and verify that all affected user groups have/had appropriate representation.

• Verify that project initiation and cost have received proper management approval.

• Review the conceptual design specifications (e.g., transforms, data descriptions) to ensure that they address the needs of the user.

• Review the conceptual design to ensure that control specifications have been defined.

• Determine whether a reasonable number of vendors received a proposal covering the project scope and user requirements.

• Review the UAT specification.

• Determine whether the application is a candidate for the use of an embedded audit routine. If so, request that the routine be incorporated in the conceptual design of the system.

3.3 SYSTEM DEVELOPMENT METHODOLOGIES

A systems development methodology is a structure that an organization uses to plan and control the development of information systems and software and new business applications. In the face of increasing system complexity and the need to implement new systems more quickly to achieve benefits before the business changes, system and software development practitioners have adopted many ways of organizing information system and software projects.

3.3.1 BUSINESS APPLICATION DEVELOPMENT

Business application development is part of a life cycle process with defined phases applicable to deployment, maintenance and retirement. In this process, each phase is an incremental step that lays the foundation for the next phase,

to ensure effective management control in building and operating business application systems.

A business application system developed will fall in one of two major categories:

• **Organization-centric**—The objective of organization-centric applications is to collect, collate, store, archive and share information with business users and various applicable support functions on a need-to-know basis.

Thus, sales data are made available to accounts, administration, governmental levy payment departments, etc. Regulatory levy fulfillment (i.e., tax compliance) is also addressed by the presence of organization-centric applications. Organization-centric application projects usually use the SDLC or other, more detailed software engineering approaches for development.

• **End-user-centric**—The objective of an end-user-centric application is to provide different views of data for their performance optimization. This objective includes decision support systems (DSSs) and geographic information systems (GISs). Most of these applications are developed using alternative development approaches.

A business application development project is generally initiated as a result of one or more of the following situations:

• A new opportunity that relates to a new or existing business process

• A problem that relates to an existing business process

• A new opportunity that will enable the organization to take advantage of technology

• A problem with the current technology

• Alignment of business applications with business partners/industry standard systems and respective interfaces

All these situations are tightly coupled with key business drivers, which are defined as the attributes of a business function that drive the behavior and implementation of that business function to achieve the strategic business goals. Thus, all critical business objectives (as a breakdown of the organizational strategy) have to be translated into key business drivers for all parties involved in business operations during a systems development project.

Objectives should be SMART (see section 3.1.9, Project Objectives) so that general requirements will be expressed in a scorecard form, which allows

objective evidence to be collected in order to measure the business value of an application and to prioritize requirements. A key benefit of this approach is that all affected parties will have a common and clear understanding of the objectives and how they contribute to business support. Additionally, conflicting key business drivers (e.g., cost versus functionality) and mutually dependent key business drivers can be detected and resolved in early stages of the project.

Business application projects should be initiated using well-defined procedures or activities as part of a defined process to communicate business needs to management. These procedures often require detailed documentation identifying the need or problem, specifying the desired solution and relating the potential benefits to an organization. All internal and external factors affected by the problem and their effect on an organization should be identified.

3.3.2 SDLC MODELS

Several different SDLC models exist, including:

• Traditional waterfall

• V-shaped

• Iterative

A **traditional SDLC (waterfall) model** and variants of the model normally involve a life cycle verification approach that ensures that potential mistakes are corrected early and not solely during final acceptance testing. This life cycle approach is the oldest and most widely commonly used for developing business applications. This approach works best when a project’s requirements are likely to be stable and well defined. It facilitates the determination of a system architecture relatively early in the development effort. The approach is based on a systematic, sequential approach to system and/or software development. The traditional approach is useful in web applications in which prototypes of screens are necessary to aid in the completion of requirements and design.

The primary advantage of the traditional approach is that it provides a template into which methods for the requirements (i.e., definition, design, programming, etc.) can be placed. However, some of the problems

encountered with this approach include the following:

• Unanticipated events that result in iterations, creating problems in implementing the approach

• The difficulty of obtaining an explicit set of requirements from the customer/user as the approach requires

• Managing requirements and convincing the user about the undue or unwarranted requirements in the system functionality, which may lead to conflict in the project

• The necessity of customer/user patience, which is required because under this approach a working version of the system's programs will not be available until late in the project's life cycle

• A changing business environment that alters or changes the customer/user requirements before they are delivered

A **verification and validation model**, also called the V-model, also emphasizes the relationship between development phases and testing levels

(figure 3.10). The most granular testing—the unit test—occurs immediately after programs have been written. Following this model, testing occurs to validate the detailed design. System testing relates to the architectural specification of the system while final UAT references the requirements.

From an IS auditor's perspective, the V-model's defined life cycle phases and specific points for review and evaluation provide the following advantages:

• An IS auditor's influence is significantly increased when there are formal procedures and guidelines identifying each phase in the business application life cycle and the extent of IS auditor involvement.

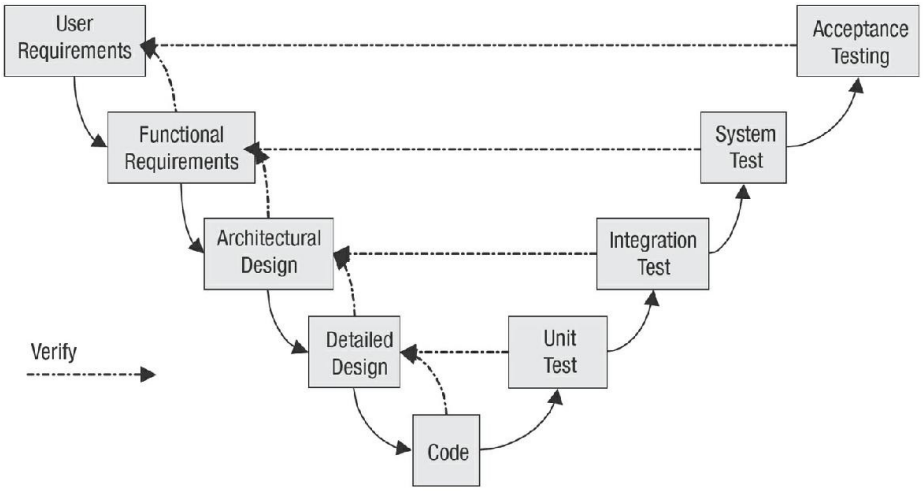
• An IS auditor can review all relevant areas and phases of the systems development project and report independently to management on the adherence to planned objectives and organizational procedures.

• An IS auditor can identify selected parts of the system and become involved in the technical aspects on the basis of his/her skills and abilities.

• An IS auditor can provide an evaluation of the methods and techniques applied

through the development phases of the business application life

Figure 3.10—Verification and Validation



cycle.

The **iterative model** is a cyclical process in which business requirements are developed and tested in iterations until the entire application is designed, built and tested. During each iteration, the development process goes through each phase, from requirements through testing, and each subsequent cycle incrementally improves the process.

Note: A CISA candidate should understand systems development models and how they are used to evaluate the existence and effectiveness of critical system development controls. A CISA candidate should also understand how a selected methodology is used and whether the process will properly address the project requirements.

3.3.3 SDLC PHASES

An SDLC approach is made up of a number of distinct phases (**figure 3.11**), each with a defined set of activities and outcomes. Each phase has defined goals and activities to perform with assigned responsibilities, expected outcomes and target completion dates. There are other interpretations that use a slightly different number of phases with different names.

The actual phases for each project may vary depending on whether a

developed or acquired solution is chosen. For example, system maintenance efforts may not require the same level of detail or number of phases as new applications. The phases and deliverables should be decided during the early planning stages of the project.

Over the years, business application development has occurred largely through the use of traditional SDLC phases. As purchased packages have become more common, the design and development phases of the traditional life cycle are being replaced with selection and configuration phases.

The content that follows describes each phase, its purpose and relationship to prior phases, the general activities performed and expected outcomes.

Phase 1—Feasibility Study

A feasibility study is concerned with analyzing the benefits and solutions for the identified problem area. This study includes development of a business case that states the strategic benefits of implementing the system either in productivity gains or in future cost avoidance, identifies and quantifies the cost savings of the new system, and estimates a payback schedule for the cost incurred in implementing the system or shows the projected ROI.

Figure 3.11—Traditional System Development Life Cycle Approach SDLC Phase

General Description

Phase 1—Feasibility Study

Determine the strategic benefits of implementing the system either in productivity gains or in future cost avoidance, identify and quantify the cost savings of a new system, and estimate a payback schedule for costs incurred in implementing the system. Further, intangible factors such as readiness of the business users and maturity of the business processes will also be considered and assessed. This business case provides the justification for proceeding to the next phase.

Phase 2—Requirements

Define the problem or need that requires resolution and define the Definition

functional and quality requirements of the solution system. This can be either a customized approach or vendor-supplied software

package, which would entail following a defined and documented

acquisition process. In either case, the user needs to be actively involved.

Phase 3A—Software

Based on requirements defined, prepare a request for proposal

Selection and Acquisition

outlining the entity requirements to invite bids from prospective

(*purchased systems*)

suppliers, in respect of those systems that are intended to be procured from vendors or solution providers.

Phase 3B—Design (*in-*

Based on the requirements defined, establish a baseline of system and *house development*)

subsystem specifications that describe the parts of the system, how they interface, and how the system will be implemented using the chosen hardware, software and network facilities. Generally, the design also includes program and database specifications and will address any security considerations. Additionally, a formal change control process is established to prevent uncontrolled entry of new requirements into the development process.

Phase 4A—Configuration

Configure the system, if it is a packaged system, to tailor it to the (*purchased systems*)

organization’s requirements. This is best done through the

configuration of system control parameters, rather than changing program code. Modern software packages are extremely flexible,

making it possible for one package to suit many organizations simply by switching functionality on or off and setting parameters in tables.

There may be a need to build interface programs that will connect the acquired system with existing programs and databases.

Phase 4B—Development

Use the design specifications to begin programming and formalizing (*in-house development*)

supporting operational processes of the system. Various levels of testing also occur in this phase to verify and validate what has been developed. This generally includes all unit and system testing and several iterations of user acceptance testing.

Phase 5—Final Testing and

Establish the actual operation of the new information system, with the Implementation

final iteration of user acceptance testing and user sign-off conducted in this phase. The system also may go through a certification and accreditation process to assess the effectiveness of the business application in mitigating risk to an appropriate level and providing management accountability over the effectiveness of the system in meeting its intended objectives and in establishing an appropriate level of internal control.

Phase 6—Post-

Following the successful implementation of a new or extensively

implementation

modified system, implement a formal process that assesses the

adequacy of the system and projected cost-benefit or ROI

measurements vis-à-vis the feasibility stage findings and deviations.

In so doing, IS project and end-user management can provide lessons learned and/or plans for addressing system deficiencies as well as recommendations for future projects regarding system development and project management processes followed.

Intangible benefits such as improved morale may also be identified; however, benefits should be quantified whenever possible.

A feasibility study achieves the following:

• Defines a time frame for the implementation of the required solution

• Determines an optimum alternative risk-based solution for meeting business needs and general information resource requirements (e.g., whether to develop or acquire a system). Such processes can easily be mapped to SDLC and rapid application development (RAD).

• Determines whether an existing system can correct the situation with slight or no modification (e.g., workaround)

• Determines whether a vendor product offers a solution to the problem

• Determines the approximate cost to develop the system to correct the situation

• Determines whether the solution fits the business strategy Factors impacting whether to develop or acquire a system include the following:

• The date the system needs to be functional

• The cost to develop the system as opposed to buying it

• The resources, staff (availability and skill sets) and hardware required to develop the system or implement a vendor solution

• In a vendor system, the license characteristics (e.g., yearly renewal, perpetual) and maintenance costs

• The other systems needing to supply information to or use information from the vendor system that will need the ability to interface with the system

• Compatibility with strategic business plans

• Compatibility with risk appetite and regulatory compliance needs

• Compatibility with the organization's IT infrastructure

• Likely future requirements for changes to functionality offered by the system

The result of the completed feasibility study should be a comparative report that shows the results of criteria analyzed (e.g., costs, benefits, risk, resources required and organizational impact) and recommends one of the

alternatives/solutions and a course of action.

Closely related to a feasibility study is the development of an impact assessment. An impact assessment is a study of the potential future effects of

a development project on current projects and resources. The resulting document should list the pros and cons of pursuing a specific course of action.

Phase 2—Requirements Definition

Requirements definition is concerned with identifying and specifying the business requirements of the system chosen for development during the feasibility study. Requirements include descriptions of:

• What a system should do

• How users will interact with a system

• Conditions under which the system will operate

• Information criteria the system should meet

This phase also deals with overarching issues that are sometimes called nonfunctional requirements (e.g., access control). Many IT security weaknesses can be corrected with a more critical focus on security within the context of the SDLC and, in particular, during the requirements definition.

To successfully complete the requirements definition phase, the project team should perform the following activities:

• Identify and consult stakeholders to determine their requirements.

• Analyze requirements to detect and correct conflicts (mainly, differences between requirements and expectations) and determine priorities.

• Identify system bounds and how the system should interact with its environment.

• Identify any relevant security requirements.

• Convert user requirements into system requirements (e.g., an interactive user interface prototype that demonstrates the screen look and feel).

• Record requirements in a structured format. Historically, requirements have been recorded in a written requirements specification, possibly

supplemented by some schematic models. Commercial requirements

management tools now are available that allow requirements and related information to be stored in a multiuser database.

• Verify that requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable. Because of the high cost of rectifying requirements' problems in downstream development phases, effective

requirements reviews have a large payoff.

• Resolve conflicts between stakeholders.

• Resolve conflicts between the requirements set and the resources that are available.

The users in this process specify their information resource needs and how they wish to have them addressed by the system (e.g., access controls, regulatory requirements, management information needs and interface requirements).

From this interactive process, a general preliminary design of the system may be developed and presented to user management for review and approval. A project schedule is created for developing, testing and implementing the system. Also, commitments are obtained from the system's developers and affected user departments to contribute the necessary resources to complete the project. It is important to note that all management and user groups must be actively involved in the requirements definition phase to prevent problems such as expending resources on a system that will not satisfy the business requirements. User involvement is necessary to obtain commitment and full benefit from the system. Without management sponsorship, clearly defined requirements and user involvement, the benefits may never be realized.

An IS auditor should pay close attention to the degree the organization's system security engineering team is involved in the development of security controls throughout the data life cycle within the business application. This means the controls are in place regarding applicable confidentiality, integrity and availability of data from creation/receipt to processing, storage, transmission and, ultimately, destruction. This includes whether adequate audit trails are defined as part of the system because these affect the auditor's ability to identify issues for proper follow-up. The IS auditor may also identify regulatory, statutory and legal requirements for the solution being developed.

Phase 3A—Software Selection and Acquisition

At this point in the project, it may be appropriate to evaluate the risk and benefits of developing a new system versus acquiring from a vendor a

suitable system that is complete, tested and proven. Consideration should be given to the ability of the organization to undertake the proposed development project, the costs and risk of doing so, and the benefits of having total ownership and control over the new system rather than becoming dependent on a vendor.

Software acquisition is not a phase in the standard SDLC. However, if a decision is reached to acquire rather than develop software, software acquisition is the process that should occur after the requirements definition phase. The decision is generally based on various factors such as the cost differential between development and acquisition, availability of generic software, and the time gap between development and acquisition. Please note that if the result of the decision to develop/acquire is to purchase a vendor-supplied software package, the user must be actively involved in the package evaluation and selection process.

Phase 3B—Design

Based on the general preliminary design and user requirements defined in the requirements definition phase, a detailed design should be developed.

Generally, a programming and analyst team is assigned the tasks of defining the software architecture (depicting a general blueprint of the system) and then detailing or decomposing the system into its constituent parts such as modules and components. This approach is an enabler for effective allocation of resources to design the system and define how the system will satisfy all its information requirements. Depending on the complexity of the system, several iterations in defining system-level specifications may be needed to get down to the level of detail necessary to start development activities such as coding.

Key design phase activities include the following:

• Developing system flowcharts and entity relationship models to illustrate how information will flow through the system

• Determining the use of structured design techniques (which are processes to define applications through a series of data or process flow diagrams) that show various relationships from the top level down to the details

• Describing inputs and outputs such as screen designs and reports. If a prototyping tool is going to be used, it is most often used in the screen design and presentation process (via online programming facilities) as part

of an integrated development environment.

• Determining processing steps and computation rules when addressing

functional requirement needs

• Determining data file or database system file design

• Preparing program specifications for various types of requirements or information criteria defined

• Developing test plans for the various levels of testing:

– Unit (program)

– Subsystem (module)

– Integration (system)

– Interface with other systems

– Loading and initializing files

– Stress

– Security

– Backup and recovery

• Developing data conversion plans to convert data and manual procedures from the old system to the new system. Detailed conversion plans will alleviate implementation problems that arise due to incompatible data, insufficient resources or staff who are unfamiliar with the operations of the new system.

• Performing a risk assessment of information flows

Risk Associated With Software Development

There are many potential types of risk that can occur when designing and developing software systems, including the following:

• **Strategic risk** arises when the business goals are identified and weighted without taking the corporate strategy into account. The strategic importance of the business goals depends on the strategic importance of the related business area.

• **Business risk** (or benefit risk) relates to the likelihood that the new system may not meet the users' business needs, requirements and expectations. For example, the business requirements that were to be addressed by the new system are still unfulfilled, and the process has been a waste of resources.

In such a case, even if the system is implemented, it will most likely be underutilized and not maintained, making it obsolete in a short period of time.

• **Project risk** (or delivery risk) arises if the project activities to design and develop the system exceed the limits of the financial resources set aside for the project and, as a result, the project may be completed late, if ever.

Software project risk exists at multiple levels:

– Within the project (e.g., risk associated with not identifying the right requirements to deal with the business problem or opportunity that the system is meant to address and not managing the project to deliver within time and cost constraints)

– With suppliers (e.g., risk associated with a failure to clearly communicate requirements and expectations, resulting in suppliers delivering late, at more than the expected cost and/or with deficient quality)

– Within the organization (e.g., risk associated with stakeholders not providing needed inputs or committing resources to the project, and changing organizational priorities and politics)

– With the external environment (e.g., risk associated with impacts on the projects caused by the actions and changing preferences of customers, competitors, government/regulators and economic conditions)

– With the technology chosen (e.g., sudden displacement of technology chosen by a one more cost-efficient; insufficient compatibility in the marketplace, resulting in barriers to potential clients' use of the new system)

The primary cause of these problems is a lack of discipline in managing the software development process or the use of a methodology inappropriate to the system being developed. In such instances, an organization is not providing the infrastructure and support necessary to help projects avoid these problems. In such cases, successful projects, if occurring, are not repeatable, and SDLC

activities are not defined and followed adequately (i.e., insufficient maturity). However, with effective management, SDLC

management activities can be controlled, measured and improved.

An IS auditor should be aware that merely following an SDLC management approach does not ensure the successful completion of a development project.

An IS auditor should also review the management discipline over a project related to the following:

• The project meets cooperative goals and objectives.

• Project planning is performed, including effective estimates of resources, budget and time.

• Scope creep is controlled and there is a software baseline to prevent requirements from being added into the software design or having an uncontrolled development process.

• Management is tracking software design and development activities.

• Senior management support is provided to the software project's design and development efforts.

• Periodic review and risk analysis are performed in each project phase.

Use of Structured Analysis, Design and Development Techniques

The use of structured analysis, design and development techniques is closely associated with the traditional, classic SDLC approach to software development. These techniques provide a framework for identifying and representing the data and process components of an application using various graphic notations at different levels of abstraction, until the abstraction level that enables programmers to code the system is reached. Early on, for example, the following activities occur in defining the requirements for a new system:

• Develop system context diagrams (e.g., high-level business process flow schema).

• Perform hierarchical data flow/control flow decomposition.

• Develop control transformations.

• Develop mini-specifications.

• Develop data dictionaries.

• Define all external events—inputs from external environment.

• Define single transformation data flow diagrams (DFDs) from each external event.

The next level of design provides greater detail for building the system, including developing system flowcharts, inputs/outputs, processing steps and computations, and program and data file or database specifications. It should be noted that representation of functions is developed in a modularized top-down fashion. This enables programmers to systematically develop and test modules in a linear fashion.

An IS auditor should be particularly concerned with whether the processes under a structured approach are well defined, documented and followed when using the traditional SDLC approach to business application development.

Entity Relationship Diagrams

An important tool in the creation of a general preliminary design is the use of entity relationship diagrams (ERDs). An ERD depicts a system's data and how these data interrelate. An ERD can be used as a requirements analysis tool to obtain an understanding of the data a system needs to capture and manage. In this case, the ERD represents a logical data model. An ERD can also be used later in the development cycle as a design tool that helps document the actual database schema that will be implemented. Used in this way, the ERD represents a physical data model.

As the name suggests, the essential components of an ERD are entities and relationships. Entities are groupings of like data elements or instances that may represent actual physical objects or logical constructs. An entity is described by attributes, which are properties or characteristics common to all or some of the instances of the entity. Particular attributes, either singularly or in combination,

form the keys of an entity. An entity's primary key uniquely identifies each instance of the entity. Entities are represented on ERDs as rectangular boxes with an identifying name.

Relationships depict how two entities are associated (and, in some cases, how instances of the same entity are associated). The classic way of depicting a relationship is a diamond with connecting lines to each related entity. The name in the diamond describes the nature of the relationship. The relationship may also specify the foreign key attributes that achieve the association among the entities. A foreign key is one or more attributes held in one entity that map to the primary key of a related entity.

Software Baselining

The software design phase represents the optimum point for software baselining to occur. The term software baseline means the cutoff point in the design and is also referred to as design freeze. User requirements are reviewed, item by item, and considered in terms of time and cost. The

changes are undertaken after considering various types of risk, and change does not occur without undergoing formal strict procedures for approval based on a cost-benefit impact analysis. Failure to adequately manage the requirements for a system through baselining can result in a number of types of risk. Foremost among these is scope creep—the process through which requirements change during development.

Software baselining also relates to the point when formal establishment of the software configuration management process occurs. At this point, software work products are established as configuration baselines with version numbers. This includes functional requirements, specifications and test plans.

All of these work products are configuration items and are identified and brought under formal change management control. This process will be used throughout the application system's life cycle, where SDLC procedures for analysis, design, development, testing and deployment are enforced on new requirements or changes to existing requirements.

User Involvement in the Design

After business processes have been documented and it is understood how those

processes might be executed in a new system, involvement of users during the design phase is limited. Given the technical discussion that usually occurs during a design review, end-user participation in the review of detailed design work products is normally not appropriate. However, developers should be able to explain how the software architecture will satisfy system requirements and outline the rationale for key design decisions. Choices of particular hardware and software configurations may have cost implications of which stakeholders need to be aware and control implications that are of interest to an IS auditor.

After the detailed design has been completed, including user approvals and software baselining, the design is distributed to the system developers for coding.

IS Auditor's Role in Project Design

The IS auditor is primarily focused on whether an adequate system of controls is incorporated into system specifications and test plans, and whether

continuous online auditing functions are built into the system (particularly for ecommerce applications and other types of paperless environments).

Additionally, an IS auditor is interested in evaluating the effectiveness of the design process itself (such as in the use of structured design techniques, prototyping and test plans, and software baselining) to establish a formal software change process that effectively freezes the inclusion of any changes to system requirements without a formal review and approval process. The key documents coming out of this phase include system, subsystem, program and database specifications, test plans, and a defined and documented formal software change control process.

An IS auditor should perform the following functions:

• Review the system flowcharts for adherence to the general design. Verify that appropriate approvals were obtained for any changes and all changes were discussed and approved by appropriate user management.

• Review for appropriateness the input, processing and output controls designed into the system.

• Interview the key users of the system to determine their understanding of how

the system will operate and assess their level of input into the design of screen formats and output reports.

• Assess the adequacy of audit trails to provide traceability and accountability of system transactions.

• Verify the integrity of key calculations and processes.

• Verify that the system can identify and process erroneous data correctly.

• Review the quality assurance results of the programs developed during this phase.

• Verify that all recommended corrections to programming errors were made and the recommended audit trails or embedded audit modules (EAMs) were coded into the appropriate programs.

• Perform a risk assessment.

Phase 4A—Configuration

System configuration, as it relates to the SDLC, consists of defining, tracking and controlling changes in an acquired system to meet the needs of the business. For ERP systems, the task often involves the modification of configuration tables as well as some development, primarily to ensure that

the ERP system is integrated into the existing IT architecture. System configuration is supported by the change management policies and processes, which define:

• Roles and responsibilities

• Classification and prioritization of all changes based on business risk

• Assessment of impact

• Authorization and approval of all changes by the business process owners and IT

• Tracking and status of changes

• Impact on data integrity (e.g., all changes to data files being made under system and application control rather than by direct user intervention) **Phase 4B —Development**

The development phase uses the detailed design developed in phase 3B.

Responsibilities in this phase rest primarily with programmers and systems analysts who are building the system. Key activities performed in a test/development environment include:

• Coding and developing program and system-level documents

• Debugging and testing the programs developed

• Developing programs to convert data from the old system for use on the new system

• Creating user procedures to handle transition to the new system

• Training selected users on the new system because their participation will be needed

• Ensuring modifications are documented and applied accurately and completely to vendor-acquired software to ensure that future updated versions of the vendor's code can be applied

• Identifying secure coding and configuration standards

Programming Methods and Techniques

To enhance the quality of programming activities and future maintenance capabilities, program coding standards should be applied. Program coding standards are essential to writing, reading and understanding code, simply and clearly, without having to refer back to design specifications. Elements of program coding standards include methods and techniques for internal (source-code level) documentation, methods for data declaration, and an

approach to statement construction and techniques for input/output (I/O). The programming standards applied are an essential control because they serve as a method of communicating among members of the program team, and between

the team and users during system development. Program coding standards minimize system development setbacks resulting from personnel turnover, provide the material needed to use the system effectively, and are required for efficient program maintenance and modifications.

Additionally, traditional structured programming techniques should be applied in developing quality and easily maintained software products. They are a natural progression from the top-down structuring design techniques previously described. Like the design specifications, structured application programs are easier to develop, understand and maintain because they are divided into subsystems, components, modules, programs, subroutines and units. Generally, the greater the extent to which each software item described performs a single, dedicated function (cohesion) and retains independence from other comparable items (coupling), the easier it is to maintain and enhance a system because it is easier to determine where and how to apply a change and reduce the chances of unintended consequences.

Online Programming Facilities (Integrated Development Environment)

To facilitate effective use of structured programming methods and techniques, an online programming facility should be available as part of an integrated development environment (IDE). This allows programmers to code and compile programs interactively with a remote computer or server from a terminal or a client's PC workstation. Through this facility, programmers can enter, modify and delete programming codes as well as compile, store and list programs (source and object) on the development computer. The online facilities can also be used by non-IS staff to update and retrieve data directly from computer files.

Online programming facilities are used on PC workstations. The program library is on a server, such as a mainframe library management system, but the modification/development and testing are performed on the workstation.

This approach can lower the development costs, maintain rapid response time, and expand the programming resources and aids available (e.g., editing

tools, programming languages, debugging aids). From the perspective of control, this approach introduces the potential weaknesses of:

• The proliferation of multiple versions of programs

• Reduced program and processing integrity through the increased potential for unauthorized access and updating

• The possibility that valid changes could be overwritten by other changes In general, an online programming facility allows faster program development and helps to enforce the use of standards and structured programming techniques. Online systems improve the programmer's

problem-solving abilities, but online systems create vulnerabilities resulting from unauthorized access. Access control software should be used to help reduce the risk.

Programming Languages

Application programs must first be coded in statements, instructions or a programming language that is easy for a programmer to write and that can be read by the computer. These statements (source code) will then be translated by the language translator/compiler into a binary machine code or machine language (object code) that the computer can execute.

Programming languages commonly used for developing application programs include the following:

• High-level, general-purpose programming languages such as COBOL and the C programming language

• Object-oriented languages for business purposes such as C++, Eiffel and Java

• IDEs such as Visual Studio or JBuilder, which provide coding templates automatically

• Web scripting languages (e.g., Hypertext Markup Language [HTML], Javascript, Cascading Style Sheets [CSS])

• Data-centric programming languages (e.g., R, Scala, IDL, SAS)

• Scripting languages such as shell, Perl, Tcl, Python, JavaScript and VBScript. In web development, scripting languages are used commonly to write common gateway interface (CGI) scripts that are used to extend the functionality of web server application software (e.g., to interface with

search engines, create dynamic web pages and respond to user input).

• Low-level assembler languages designed for a specific processor type that are usually used for embedded applications (e.g., slot machines, vending machines, aerospace devices)

• Fourth-generation, high-level programming languages (4GLs), which consist of a database management system (DBMS), embedded database manager, and a nonprocedural report and screen generation facility. 4GLs provide fast iteration through successive designs. Examples of 4GLs include FOCUS, Natural and dBase.

• Decision support or expert systems languages (e.g., EXPRESS, Lisp and Prolog)

Program Debugging

Many programming bugs are detected during the system development process, after a programmer runs a program in the test environment. The purpose of debugging programs during system development is to ensure that all program abends (unplanned ending of a program due to programming errors) and program coding flaws are detected and corrected before the final program goes into production. A debugging tool is a program that will assist a programmer in debugging, fixing or fine-tuning the program under development. Compilers have some potential to provide feedback to a programmer, but they are not considered debugging tools. Debugging tools fall into three main categories:

• **Logic path monitors**—Report on the sequence of events performed by the program, thus providing the programmer with clues on logic errors

• **Memory dumps**—Provide a picture of the internal memory's content at one point in time. This is often produced at the point where the program fails or is aborted, providing the programmer with clues on inconsistencies in data or parameter values. A variant, called a trace, will do the same at different stages in the program execution to show changes in machine-level structures such as counters and registers.

• **Output analyzers**—Help check results of program execution for accuracy.

This is achieved by comparing expected results with the actual results.

Phase 5—Final Testing and Implementation

During the implementation phase, the actual operation of the new information

system is established and tested. Final UAT is conducted in this environment.

The system may also go through a certification and accreditation process to assess the business application's effectiveness at mitigating risk to an appropriate level and provide management accountability over the effectiveness of the system in meeting its intended objectives and establishing an appropriate level of internal control.

After a successful full-system testing, the system is ready to migrate to the production environment. The programs have been tested and refined; program procedures and production schedules are in place; all necessary data have been successfully converted and loaded into the new system; and the users have developed procedures and been fully trained in the use of the new system. A date for system migration is determined and production turnover takes place. In the case of large organizations and complex systems, this may involve a project in itself and require a phased approach.

Planning for the implementation should begin well in advance of the actual implementation date, and a formal implementation plan should be

constructed in the design phase and revised accordingly as development progresses. Each step in setting up the production environment should be stipulated, including who will be responsible, how the step will be verified and the backout procedure if problems are experienced. If the new system will interface with other systems or is distributed across multiple platforms, some final commissioning tests of the production environment may be desirable to prove end-to-end connectivity. If such tests are run, care will be needed to ensure test transactions do not remain in production databases or files.

In the case of acquired software, the implementation project should be coordinated by user management with the help of IS management, if required. The total process should not be delegated to the vendor, to avoid possible unauthorized changes or introduction of malicious code by the vendor's employees/representatives.

After operations are established, the next step is to perform site acceptance

testing, which is a full-system test conducted on the actual operations

environment. UAT supports the process of ensuring that the system is production-ready and satisfies all documented requirements. A security test, such as a penetration test, may also be performed at this stage.

Phase 6—Post-implementation Review

Following the successful implementation of a new or extensively modified system, it is beneficial to verify the system has been properly designed and developed and that proper controls have been built into the system. A postimplementation review should meet the following objectives:

• Assessing the adequacy of the system

– Does the system meet user requirements and business objectives?

– Have access controls been adequately defined and implemented?

• Evaluating the projected cost benefits or ROI measurements

• Developing recommendations that address the system's inadequacies and deficiencies

• Developing a plan for implementing the recommendations

• Assessing the development project process

– Were the chosen methodologies, standards and techniques followed?

– Were appropriate project management techniques used?

3.3.4 IS AUDITOR'S ROLE IN SDLC PROJECT

MANAGEMENT

Throughout the project management process an IS auditor should analyze the associated risk and exposures inherent in each phase of the SDLC and ensure that the appropriate control mechanisms are in place to minimize risk in a cost-effective manner. Caution should be exercised to avoid recommending controls that cost more to administer than the associated risk they are designed to

minimize.

When reviewing the SDLC process, an IS auditor should obtain

documentation from the various phases and attend project team meetings, offering advice to the project team throughout the system development process. An IS auditor should also assess the project team's ability to produce key deliverables by the promised dates.

Typically, an IS auditor should review the adequacy of the following project

management activities:

• Levels of oversight by project committee/board

• Risk management methods within the project

• Issue management

• Cost management

• Processes for planning and dependency management

• Reporting processes to senior management

• Change control processes

• Stakeholder management involvement

• Sign-off process (at a minimum, signed approvals from systems development and user management responsible for the cost of the project and/or use of the system)

Additionally, adequate and complete documentation of all phases of the SDLC process should be evident. Typical types of documentation include, but should not be limited to, the following:

• Objectives defining what is to be accomplished during that phase

• Key deliverables by phases with project personnel assigned direct responsibilities for these deliverables

• A project schedule with highlighted dates for the completion of key deliverables

• An economic forecast for that phase, defining resources and the cost of the resources required to complete the phase

3.3.5 SOFTWARE DEVELOPMENT METHODS

There are several different methods of designing and developing a software system. The choice of a particular method is driven by considerations such as organizational policy, developer knowledge and preference, and the technology being used. The selection of a software development method is generally independent of the selection of a project organization model. An object-oriented approach could be utilized on a project organized into distinct phases, as in a traditional waterfall model of software development, as could an agile project method in which each short iteration delivers working software.

Prototyping—Evolutionary Development

Prototyping, also known as “heuristic” or “evolutionary development,” is the process of creating a system through controlled trial-and-error procedures to reduce the level of risk in developing the system. That is, it enables the developer and customer to understand and react to risk at each evolutionary level (using prototyping as a risk reduction mechanism). It combines the best features of classic SDLC by maintaining the systematic stepwise approach and incorporates it into an iterative framework that more realistically reflects the real world.

The initial emphasis during the development of the prototype is usually placed on the reports and screens, which are the system aspects most used by the end users. This allows the end user to see a working model of the proposed system within a short time. There are two basic methods or approaches to prototyping:

1. Build the model to create the design (i.e., the mechanism for defining requirements). Then, based on that model, develop the system design with all the performance, quality and maintenance features needed.

2. Gradually build the actual system that will operate in production using a 4GL that has been determined to be appropriate for the system being built.

The problem with the first approach is that there can be considerable pressure to implement an early prototype. Often, users observing a working model cannot understand why the early prototype must be refined further. The fact that the prototype needs to be expanded to handle transaction volumes, client-server network connectivity, and backup and recovery procedures, and provide for security, auditability and control is often not understood.

The second approach typically works with small applications using 4GL

tools. However, for larger efforts, it is necessary to develop a design strategy for the system even if a 4GL is used. The use of 4GL techniques alone will cause the same difficulties (e.g., poor quality, poor maintainability and low user acceptance) encountered when developing business applications using conventional approaches.

Another overall disadvantage of prototyping is that it often leads to functions or extras being added to the system that are not included in the initial

requirements document. All major enhancements beyond the initial requirements document should be reviewed to ensure that they meet the strategic needs of the organization and are cost-effective. Otherwise, the final system may be functionally rich but inefficient.

A potential risk with prototyped systems is that the finished system will have poor controls. By focusing mainly on what the user wants and what the user sees, system developers may miss some of the controls, such as backup recovery, security and audit trails, that come out of the traditional system development approach.

Change control often becomes much more complicated with prototyped systems. Changes in designs and requirements happen so quickly that they are seldom documented or approved, and the system can escalate to a point of not being maintainable.

Although an IS auditor should be aware of the risk associated with prototyping, an IS auditor should also be aware that this method of system development can provide the organization with significant time and cost savings.

Rapid Application Development

RAD is a methodology that enables an organization to develop strategically important systems quickly while reducing development costs and maintaining quality. This is achieved by using a series of proven application development techniques within a well-defined methodology. These techniques include the use of:

• Small, well-trained development teams

• Evolutionary prototypes

• Integrated power tools that support modeling, prototyping and component reusability

• A central repository

• Interactive requirements and design workshops

• Rigid limits on development time frames

RAD supports the analysis, design, development and implementation of individual application systems. However, RAD does not support the planning

or analysis required to define the information needs of the enterprise as a whole or of a major business area of the enterprise. RAD provides a means for developing systems faster while reducing cost and increasing quality. This is done by automating large portions of the SDLC, imposing rigid limits on development time frames and reusing existing components. The RAD

methodology has four major stages:

1. The **concept definition stage** defines the business functions and data subject areas that the system will support and determines the system scope.

2. The **functional design stage** uses workshops to model the system's data and processes and build a working prototype of critical system

components.

3. The **development stage** completes the construction of the physical database and application system, builds the conversion system, and develops user aids and

deployment work plans.

4. The **deployment stage** includes final-user testing and training, data conversion and the implementation of the application system.

RAD uses prototyping as its core development tool no matter which underlying technology is used. In contrast, object-oriented software development (OOSD) and data-oriented system development (DOSD) use continuously developing models but have a focus on content solution space (e.g., how to best address the problem to make the code reusable and maintainable) and can be applied using a traditional waterfall approach. It should also be noted that BPR attempts to convert an existing business process rather than make dynamic changes.

Agile Development

Agile development is an alternative method for software development.

Assuming that all requirements cannot be articulated upfront, agile approaches, such as the Scrum methodology, propose a more iterative and incremental approach instead of the sequential approach of the SDLC. Scrum aims to move planning and directing tasks from the project manager to the team, leaving the project manager to work on removing the obstacles to the team's ability to achieve its objectives. Other agile methods include Extreme Programming (XP), Crystal, Adaptive Software Development (ASD), Feature

Driven Development (FDD) and Dynamic Systems Development Method (DSDM). These processes are termed "agile" because they are designed to flexibly handle changes to the system being developed or the project that is performing the development.

Agile development processes have a number of common characteristics:

• The use of small, time-boxed subprojects or iterations. In this instance, each iteration forms the basis for planning the next iteration.

• Replanning the project at the end of each iteration (referred to as a "sprint"

in Scrum), including reprioritizing requirements, identifying any new requirements and determining within which release delivered functionality should be implemented

• Relatively greater reliance, compared to traditional methods, on tacit knowledge—the knowledge in people's heads—as opposed to external knowledge that is captured in project documentation

• A heavy influence on mechanisms to effectively disseminate tacit knowledge and promote teamwork. Therefore, teams are kept small in size, comprise both business and technical representatives, and are located physically together. Team meetings to verbally discuss progress and issues occur daily, but with strict time limits.

• At least some of the agile methods stipulate pair-wise programming (two persons code the same part of the system) as a means of sharing knowledge and as a quality check.

• A change in the role of the project manager, from one primarily concerned with planning the project, allocating tasks and monitoring progress to that of a facilitator and advocate. Responsibility for planning and control is delegated to the team members.

Agile development does not ignore the concerns of traditional software development but approaches them from a different perspective. Agile development:

• Only plans for the next iteration in detail, rather than planning subsequent development phases.

• Uses an adaptive approach to requirements and does not emphasize managing a requirements baseline.

• Focuses on quickly proving an architecture by building actual functionality

versus formally defining, early on, software and data architecture in increasingly more detailed models and descriptions.

• Assumes limits to defect testing but attempts to validate functions through a frequent-build test cycle and correct problems in the next subproject before too much time and cost are incurred.

• Does not emphasize defined and repeatable processes, but instead performs and adapts its development based on frequent inspections.

Object-oriented System Development

OOSD is the process of solution specification and modeling in which data and procedures can be grouped into an entity known as an object. An object's data are referred to as its attributes and its functionality is referred to as its methods. This contrasts with the traditional (structured SDLC) approach that considers data separately from the procedures that act on them (e.g., program and database specifications). Proponents of OOSD claim the combination of data and functionality is aligned with how humans conceptualize everyday objects.

OOSD is a programming technique, not a software development

methodology. OOSD can be done while following any of the widely diverse set of software methodologies. A particular programming language or use of a particular programming technique does not imply or require use of a particular software development methodology.

Objects usually are created from a general template called a "class." The template contains the characteristics of the class without containing the specific data that need to be inserted into the template to form the object.

Classes are the basis for most design work in objects. Classes are either superclasses (i.e., root or parent classes) with a set of basic attributes or methods or subclasses, which inherit the characteristics of the parent class and may add (or remove) functionality as required. In addition to inheritance, classes may interact through sharing data, referred to as aggregate or component grouping, or sharing objects.

Aggregate classes interact through messages, which are requests for services from one class (called a client) to another class (called a server). The ability

of two or more objects to interpret a message differently at execution, depending on the superclass of the calling object, is termed "polymorphism."

To realize the full benefits of using object-oriented programming, it is necessary to employ object-oriented analysis and design approaches. Dealing with objects should permit analysts, developers and programmers to consider larger logical chunks of a system and clarify the programming process.

The major advantages of OOSD are as follows:

• The ability to manage an unrestricted variety of data types

• Provision of a means to model complex relationships

• The capacity to meet the demands of a changing environment A significant development in OOSD is the use of Unified Modeling Language (UML). UML is a general-purpose notational language for specifying and visualizing complex software for large object-oriented projects, but it may be used for other purposes. This signals a maturation of the object-oriented development approach. While object-orientation is not yet pervasive, it can accurately be said to have entered the computing mainstream. Applications that use object-oriented technology are:

• Web applications

• Ebusiness applications

• Computer-aided software engineering (CASE) for software development

• Office automation for email and work orders

• Artificial intelligence (AI)

• Computer-assisted manufacturing (CAM) for production and process control

Component-based Development

Component-based development can be regarded as an outgrowth of object-oriented development. Component-based development means assembling applications from cooperating packages of executable software that make their services available through defined interfaces (i.e., enabling pieces of programs called “objects,” to communicate with one another regardless of the programming language in which they were written or what OS they are running). The basic types of components are:

• **In-process client components**—These components must run from within a parent/host container such as a mobile application, a virtual machine appliance or an applet.

• **Stand-alone client components**—Applications that expose services to other software can be used as components. Well-known examples are Microsoft’s

Excel and Word.

• **Stand-alone server components**—Processes running on servers that provide services in standardized ways can be components by means of web application frameworks, application servers, web services, Lightweight Directory Access Protocol (LDAP) directory services, etc.

• **In-process server components**—These components run on servers within containers. Examples include Microsoft's Transaction Server (MTS) and Oracle's JavaBeans.

Tool developers support one or another of these standards with powerful visual tools now available for designing and testing component-based applications. Additionally, a growing number of commercially available application servers support MTS or Enterprise Java Beans (EJB). There is a growing market for third-party components. A primary benefit of component-based development is the ability to buy proven, tested software from commercial developers. The range of components available has increased.

The first components were simple in concept (e.g., buttons and list boxes).

Components now provide much more diverse functionality. Databases are now available on the web to search for commercial components.

Components play a significant role in web-based applications. Applets are required to extend static HTML, ActiveX controls or Java. Both technologies are compatible with component development.

Component-based development:

• **Reduces development time**—If an application system can be assembled from prewritten components and only code for unique parts of the system needs to be developed, then this should prove faster than writing the entire system from scratch.

• **Improves quality**—Using prewritten components means a significant percentage of the system code has been tested already.

• **Allows developers to focus more strongly on business functionality**—

An outcome of component-based development and its enabling

technologies is to further increase abstraction already achieved with high-level languages, databases and user interfaces. Developers are shielded from low-level programming details.

• **Promotes modularity**—By encouraging or forcing impassable interfaces between discrete units of functionality, it encourages modularity.

• **Simplifies reuse**—It avoids the need to be conversant with procedural or class libraries, allowing cross-language combination and allowing reusable code to be distributed in an executable format (i.e., no source is required).

(To date, large-scale reuse of business logic has not occurred.)

• **Reduces development cost**—Less effort needs to be expended on design and build. Instead, the cost of software components can be spread across multiple users.

• **Supports multiple development environments**—Components written in one language can interact with components written in other languages or running on other machines.

• **Allows a satisfactory compromise between build and buy options**—

Instead of buying a complete solution, which perhaps does not entirely fit requirements, it could be possible to purchase only needed components and incorporate these into a customized system.

To realize these advantages, attention to software integration should be provided early and continuously during the development process. No matter how efficient component-based development is, if system requirements are poorly defined or the system fails to adequately address business needs, the project will not be successful.

Web-Based Application Development

Web-based application development is an important software development approach designed to achieve easier and more effective integration of code modules within and between enterprises. Historically, software written in one

language on a particular platform has used a dedicated application programming interface (API). The use of specialized APIs has caused difficulties in integrating software modules across platforms. Technologies such as Common Object Request Broker Architecture (CORBA) and COM

that use remote procedure calls (RPCs) have been developed to allow real-time integration of code across platforms. However, using these RPC

approaches for different APIs still remains complex. Web-based application development and associated Extensible Markup Language (XML)

technologies are designed to further facilitate and standardize code module and program integration.

The other problem that web-based application development seeks to address is avoiding the need to perform redundant computing tasks with the inherent need for redundant code. One obvious example of this is a change of address notification from a customer. Instead of having to update details separately in multiple databases (e.g., contact management, accounts receivable and credit control), it is preferable for a common update process to update the multiple places required. Web services are intended to make this relatively easy to achieve.

Web application development is different from traditional third- or fourth-generation program developments in many ways—from the languages and programming techniques used, to the methodologies used to control the development work, to the way the users test and approve the development work. The risk of application development remains the same. For example, buffer overflows have been a risk since computer programming was invented (e.g., truncation issues with first-generation computer programs), because they are widely known when they could be exploited by almost anyone, almost anywhere in the world, courtesy of the Internet.

As with traditional program development, a risk-based approach should be taken in the assessment of web application vulnerabilities: Identify the business goals and supporting IT goals related to the development, then identify what can go wrong. Previous experience can be used to identify risk related to inadequate specifications, poor coding techniques, inadequate documentation, inadequate quality control (QC) and QA (including testing inadequacies), lack of proper

change control and controls over promotion into production, and so on, and put these in the context of the web application languages, development processes and deliverables (perhaps with the support of best practice material/literature on web applications development). The

focus should be on application development risk, the associated business risk and technical vulnerabilities, and how these could materialize and be controlled/addressed. Some controls will look the same for all application development activity, but many will need to reflect the way the development activity is taking place in the area under review.

With web-based application development, an XML language known as Simple Object Access Protocol (SOAP) is used to define APIs. SOAP will work with any OS and programming language that understands XML. SOAP

is simpler than using the more complex RPC-based approach, with the advantage that modules are coupled loosely so that a change to one component does not normally require changes to other components.

The second key component of web development is the Web Services

Description Language (WSDL), which is also based on XML. WSDL is used to identify the SOAP specification that is to be used for the code module API and the formats of the SOAP messages used for input and output to the code module. The WSDL is also used to identify the particular web service accessible via a corporate intranet or across the Internet by being published to a relevant intranet or Internet web server.

The final component of web services is another XML-based language—

Universal Description, Discovery and Integration (UDDI). UDDI is used to make an entry in a UDDI directory, which acts as an electronic directory accessible via a corporate intranet or across the Internet and allows interested parties to learn of the existence of available web services.

Software Reengineering

Software reengineering is a process of updating an existing system by extracting and reusing design and program components. This process is used to support major changes in the way an organization operates. A number of tools are

available to support this process. Typical methodologies used in software reengineering generally fall into the following categories:

• BPR is the thorough analysis and significant redesign of business processes and management systems to establish a better performing structure that is more responsive to the customer base and market conditions, while

yielding material cost savings.

• The service-oriented software reengineering methodology is based upon the service-oriented computer architecture, and the reengineering processes apply many concepts of RAD development leveraging responsible,

accountable, consulted and informed (RACI) charts and UML modeling.

Reverse Engineering

Reverse engineering is the process of studying and analyzing an application, a software application or a product to see how it functions and to use that information to develop a similar system. This process can be carried out in different ways:

• Decompiling object or executable code into source code and using it to analyze the program

• Black-box-testing the application to be reverse-engineered to unveil its functionality

The major advantages of reverse engineering are:

• Faster development and reduced SDLC duration

• The possibility of introducing improvements by overcoming the reverse-engineered application drawbacks An IS auditor should be aware of the following risk items:

• Software license agreements often contain clauses prohibiting the licensee from reverse engineering the software so that no trade secrets or programming techniques are compromised.

• Decompilers are relatively new tools with functions that depend on specific computers, OSs and programming languages. Any change in one of these components may require developing or purchasing a new decompiler.

DevOps

DevOps refers to the integration of development and operations processes to eliminate conflicts and barriers. This integration can create a great deal of benefits, but it can also create new risk. Decisions to adopt DevOps should be made based on factors such as an organization's climate, risk tolerance and culture and on the scope of the development project. Because DevOps changes the environment and often impacts an organization's control environment and accepted level of risk, an IS auditor should ensure that there

is a proper separation of duties.

DevOps combines the concepts of agile development, agile infrastructure and flexible operations. It requires a bridge of communication between software development and operations and the application of agile principles to all functions that support the software development life cycle. The adoption of DevOps—and, ultimately, DevSecOps in some organizations—is often closely associated with the adoption of agile. DevSecOps uses two distinctive concepts: (1) the confluence of software development, information security and IT operations groups and (2) the use of automation in those activities.

Implementing DevOps processes can be done in a logical and systematic manner and used to enhance the maturity of software development.

An organization should consider the following controls when embracing a DevOps development approach:

• Automated software scanning

• Automated vulnerability scanning

• Web application firewall

• Developer application security training

• Software dependency management

• Access and activity logging

• Documented policies and procedures

• Application performance management

• Asset management and inventorying

• Continuous auditing and/or monitoring

Business Process Reengineering and Process Change

In a generic process, some form of information enters the process, is processed, and the outcome is measured against the goal or objective of the process. The level of detail needed depends highly on the complexity of the process, the knowledge of the affected staff and the company's requirements regarding audit functionality (performance and compliance) of the process and shall fit into an existing quality management system.

Any output produced by a process must be bound to a business objective and

adhere to defined corporate standards. Monitoring of effectiveness (goal achievement), efficiency (minimum effort) and compliance must be done on a regular basis and should be included in management reports for review under the plan-do-check-act (PDCA) cycle.

BPR is the process of responding to competitive and economic pressures and customer demands to survive in the current business environment. This is usually done by automating system processes so that there are fewer manual interventions and manual controls. BPR achieved with the help of implementing an ERP system is often referred to as package-enabled reengineering (PER). Advantages of BPR are usually experienced when the reengineering process appropriately suits the business needs. BPR has increased in popularity as a method for achieving the goal of cost savings through streamlining operations.

The steps in a successful BPR are to:

• Define the areas to be reviewed.

• Develop a project plan.

• Gain an understanding of the process under review.

• Redesign and streamline the process.

• Implement and monitor the new process.

• Establish a continuous improvement process.

As a reengineering process takes hold, new results begin to emerge such as:

• New business priorities based on value and customer requirements

• A concentration on process as a means of improving product, service and profitability

• New approaches to organizing and motivating people inside and outside the enterprise

• New approaches to the use of technologies in developing, producing and delivering goods and services

• New approaches to the use of information as well as powerful and more accessible information technologies

• Refined roles for suppliers including outsourcing, joint development, quick response, just-in-time inventory and support

• Redefined roles for clients and customers, providing them with more direct

and active participation in the enterprise’s business process A successful BPR/process change project requires the project team to perform the following for the existing processes:

• Process decomposition to the lowest level required for effectively assessing a business process (typically referred to as an elementary process), which is a unit of work performed with a definitive input and output

• Identification of customers, process-based managers or process owners responsible for processes from beginning to end

• Documentation of the elementary process-related profile information including:

– Duration

– Trigger (which triggers the process to act)

– Frequency

– Effort

– Responsibility (process owner)

– Input and output

– External interfaces

– System interaction

– Risk and control information

– Performance measurement information

– Identified problematic areas and their root causes

The existing baseline processes must be documented—preferably in the form of flowcharts and related profile documents—so they can be compared to the processes after reengineering. The newly designed business processes inevitably involve changes in the way(s) of doing business and could impact the finances, philosophy and personnel of the organization; its business partners; and its customers.

Throughout the change process, the BPR team must be sensitive to organization culture, structure, direction and the components of change.

Management must also be able to predict and/or anticipate issues and problems and offer appropriate resolutions that will accelerate the change process.

BPR teams can be used to facilitate and assist the staff in transitioning into the reengineered business processes. BPR professionals are valuable in monitoring progress toward the achievement of the strategic plan of the organization.

A major concern in BPR is that key controls may be reengineered out of a business process. An IS auditor’s responsibility is to identify the existing key

controls and evaluate the impact of removing these controls. If the controls are key preventive controls, an IS auditor must ensure that management is aware of the removal of the control and is willing to accept the potential material risk of not having that preventive control.

Benchmarking Process

Benchmarking is about improving business processes. It is defined as a continuous, systematic process for evaluating the products, services or work processes of organizations recognized as world-class "references" in a globalized world. Reference products, services or processes are

systematically analyzed for one or more of the following purposes:

• Comparing and ranking

• Strategic planning; strengths, weaknesses, opportunities and threats (SWOT) analysis

• Investment decisions, company takeovers, mergers

• Product or process design or redesign/reengineering

• BPR

The following steps are conducted in a benchmarking exercise:

1. **Plan**—The benchmarking team identifies the critical processes and gains an understanding of how they are measured, the kinds of data that are needed and how the data need to be collected.

2. **Research**—The team collects baseline data about the processes of its own organization before collecting the data about other organizations. The next step is to identify the reference products or companies through sources such as business newspapers and magazines, quality award winners, trade journals, and consultants. Depending on the team's own preferences and resources, and on the marketplace, several scenarios may result:

– Benchmarks that satisfy the organization's interest already exist at no

charge from professional associations, journals or analysis firms.

– The organization may join or promote a survey launched by a single or multi-industry specialized web portal (e.g., a bookmark portal).

– The organization may conduct or subcontract business intelligence.

– The organization may enter into an agreement with one or more

“benchmark partners” who agree to share information.

Note: Based on the information gathered during the research phase, steps 3 through 6 may be skipped or adapted.

3. **Observe**—The next step is to collect data and visit the benchmarking partner. There should be an agreement with the partner organization, a data collection plan and a method to facilitate proper observation.

4. **Analyze**—This step involves summarizing and interpreting the data collected and analyzing the gaps between an organization’s process and its partner’s process. Converting key findings into new operational goals is the goal of this stage.

5. **Adopt**—Adopting the results of benchmarking can be the most difficult step. In this step, the team needs to translate the findings into a few core principles and work down from principles to strategies to action plans.

6. **Improve**—Continuous improvement is the key focus in a benchmarking exercise. Benchmarking links each process in an organization with an improvement strategy and organizational goals.

IS Auditor’s Role in Business Process Reengineering

When reviewing an organization’s BPR efforts, an IS auditor must determine whether:

• The organization’s change efforts are consistent with the overall culture and strategic plan of the organization.

• The reengineering team is trying to minimize any negative impact the change

might have on the organization’s staff.

• The BPR team has documented lessons to be learned after the completion of the BPR/process change project.

An IS auditor would also provide a statement of assurance or conclusion with

respect to the objectives of the audit.

3.3.6 SYSTEM DEVELOPMENT TOOLS AND

PRODUCTIVITY AIDS

System development tools and productivity aids include CASE applications, code generators and 4GLs.

Computer-aided Software Engineering

Application development efforts require collecting, organizing and presenting a substantial amount of data at the application, systems and program levels. A substantial amount of the application development effort involves translating this information into program logic and code for subsequent testing, modification and implementation. This often is a time-consuming process but it is necessary to develop, use and maintain computer applications.

CASE is the use of automated tools to aid in the software development process. Their use may include the application of software tools for software requirements capture and analysis, software design, code production, testing, document generation, and other software development activities.

CASE products are generally divided into three categories:

1. **Upper CASE**—Products used to describe and document business and application requirements. This information includes data object definitions and relationships, and process definitions and relationships.

2. **Middle CASE**—Products used for developing the detailed designs. These include screen and report layouts, editing criteria, data object organization and process flows. When elements or relationships change in the design, it is necessary to make only minor alterations to the automated design and all other

relationships are automatically updated.

3. **Lower CASE**—Products involved with the generation of program code and database definitions. These products use detailed design information, programming rules and database syntax rules to generate program logic, data file formats or entire applications.

Some CASE products cover two of these categories or all three of them.

CASE tools provide a uniform approach to system development, facilitate storage and retrieval of documents, and reduce the manual effort in developing and presenting system design information. This power of automation changes the nature of the development process by eliminating or combining some steps and altering the means of verifying specifications and applications.

An IS auditor needs to recognize the changes in the development process brought on by CASE. Some CASE systems allow a project team to produce a complete system from the DFDs and data elements without any traditional source code. In these situations, the DFDs and data elements become the source code.

An IS auditor should gain assurance that approvals are obtained for the appropriate specifications, users continue to be involved in the development process, and investments in CASE tools yield benefits in quality and speed.

Other key issues that an IS auditor needs to consider with CASE include the following:

• CASE tools help in the application design process but do not ensure that the design, programs and system are correct or that they fully meet the needs of the organization.

• CASE tools should complement and fit into the application development methodology, but a project methodology needs to be in place for CASE to be effective. It should be understood and used effectively by the organization’s software developers.

• The integrity of data moved between CASE products or between manual and CASE processes needs to be monitored and controlled.

• Changes to the application should be reflected in stored CASE product data.

• Just like a traditional application, application controls need to be designed.

• The CASE repository (the database that stores and organizes the documentation, models and other outputs from the different phases) needs to be secured on a need-to-know basis. Strict version control should be maintained on this database.

An IS auditor may use CASE tools as several features facilitate the audit

process. DFDs may be used as an alternative to other flowcharting techniques. In addition, CASE tools can be used to develop interrogation software and EAMs. Repository reports should be used to gain an

understanding of the system and review controls over the development process.

Code Generators

Code generators are tools that are often incorporated with CASE products, which generate program code based on parameters defined by a systems analyst or on data/entity flow diagrams developed by the design module of a CASE product. These products allow most developers to implement software programs with efficiency. An IS auditor should be aware of source code generated by such tools.

Fourth-generation Languages

4GLs are used in software development to reduce the overall effort and cost.

The common characteristics of 4GLs are:

• **Nonprocedural language**—Most 4GLs do not obey the procedural paradigm of continuous statement execution and subroutine call and control structures. Instead, they are event-driven and make extensive use of object-oriented programming concepts such as objects, properties and methods.

– For example, a COBOL programmer who wants to produce a report

sorted in a given sequence must first open and read the data file, then sort the file

and finally produce the report. A typical 4GL treats the report as an object with properties, such as input file name and sort order, and methods, such as sort file and print report.

– Care should be taken when using 4GLs. Unlike traditional languages, 4GLs can lack the lower-level detail commands necessary to perform certain types of data-intensive or online operations. These operations are usually required when developing major applications. For this reason, the use of 4GLs as development languages should be weighed carefully against traditional languages already discussed.

• **Environmental independence (portability)**—Many 4GLs are portable across computer architectures, OSs and telecommunications monitors.

Some 4GLs have been implemented on mainframe processors and

microcomputers.

• **Software facilities**—These facilities include the ability to design or paint retrieval screen formats, develop computer-aided training routines or help screens, and produce graphical outputs.

• **Programmer workbench concepts**—The programmer has access through the terminal to easy filing facilities, temporary storage, text editing and OS

commands. This type of a workbench approach is closely associated with the CASE application development approach. It is often referred to as an IDE.

• **Simple language subsets**—4GLs generally have simple language subsets that can be used by less-skilled users in an information center.

4GLs are often classified in the following ways:

• **Query and report generators**—These specialized languages can extract and produce reports (audit software). Recently, more powerful languages have been produced that can access database records, produce complex online outputs and be developed in an almost natural language.

• **Embedded database 4GLs**—These depend on self-contained database management systems. This characteristic often makes them more user-friendly

but also may lead to applications that are not integrated well with other production applications. Examples include FOCUS, RAMIS II and NOMAD 2.

• **Relational database 4GLs**—These high-level language products are usually an optional feature on a vendor's DBMS product line. These allow the applications developer to make better use of the DBMS product, but they often are not end-user-oriented. Examples include SQL+, MANTIS

and NATURAL.

• **Application generators**—These development tools generate lower-level programming languages (i.e., 3GLs) such as COBOL and C. The

application can be further tailored and customized. Data processing development personnel, not end users, use application generators.

3.3.7 INFRASTRUCTURE DEVELOPMENT/ACQUISITION PRACTICES

The physical architecture analysis, the definition of a new one and the

necessary road map to move from one to the other are critical tasks for an IT

department. Their impact is not only economic but also technological because it decides many other choices downstream, such as operational procedures, training needs, installation issues and TCO.

Conflicting requirements—such as evolving toward a services-based architecture, legacy hardware considerations, secure data access independent of data location, zero data loss and 24/7 availability—ensure that no single platform satisfies all these requirements equally. Thus, physical architecture analysis cannot be based solely on price or isolated features. A formal, reasoned choice must be made.

Information and communication technologies (ICT) departments are often tasked with making these decisions. The suggested solution must accomplish the following:

• Ensure alignment of the ICT with corporate standards.

• Provide appropriate levels of security.

• Integrate with current IT systems.

• Consider IT industry trends.

• Provide future operational flexibility to support business processes.

• Allow for projected growth in infrastructure without major upgrades.

• Include technical architecture considerations for information security, secure storage, etc.

• Ensure cost-effective, day-to-day operational support.

• Foster the usage of standardized hardware and software.

• Maximize ROI, cost transparency and operational efficiency.

Project Phases of Physical Architecture Analysis

Figure 3.12 shows the project phases to physical architecture analysis and the time at which the vendor selection process may take place.

Review of Existing Architecture

To start the process, the most current documents describing the existing architecture must be reviewed. Participants of the first workshop will be specialists of the ICT department in all areas directly impacted by physical architecture. Examples are server, storage, security and overall IT

infrastructure.

Special care must be taken in characterizing all the operational constraints that impact physical architecture such as:

• Ground issues

• Size limits

• Weight limits

• Current power supply

• Environmental operating limitations (temperature and humidity minimum and maximum)

• Physical security issues

The output of the first workshop is a list of components of the current infrastructure and constraints defining the target physical architecture.

Analysis and Design

After reviewing the existing architecture, the analysis and design of the actual physical architecture has to be undertaken, adhering to good practices and meeting business requirements.

Draft Functional Requirements

With the first physical architecture design in hand, the first (draft) of functional requirements is composed. This material is the input for the next step and the vendor selection process.

Vendor and Product Selection

While the draft functional requirements are written, the vendor selection process proceeds in parallel.

Writing Functional Requirements

After finishing the draft functional requirements and feeding the second part of this project, the functional requirements document is written and will be introduced at the second architecture workshop with staff from all affected parties. The results will be discussed and a list of the requirements that need to be refined or added will be composed.

This is the last checkpoint before the sizing and the proof of concept (POC) starts, although the planning of the POC starts after the second workshop.

With the finished functional requirements, the POC phase begins.

Proof of Concept

Establishing a POC is highly recommended to prove that the selected hardware, software and data are able to meet all expectations, including security requirements. The deliverable of the POC should be a running prototype, including the associated document and test protocols describing the tests and their results.

To start, the POC should be based on the results of the procurement phase described below in this section. For this purpose, a representative subset of the target hardware is used. The software to run the POC can be either test versions or software already supplied by the vendor; therefore, additional costs are expected to be minimal. To keep costs low, most elements of the framework are implemented in a simplified form. They will be extended to their final form in later phases.

The prototype should demonstrate the following features:

• The basic setup of the core security infrastructure

• Correct functionality of auditing components

• Basic but functional implementation of security measures as defined

• Secured transactions

• Characterization in terms of installation constraints and limits (server size, server current consumption, server weight, server room physical security)

• Performance

• Resiliency to include basic fail-over to a trusted operational state

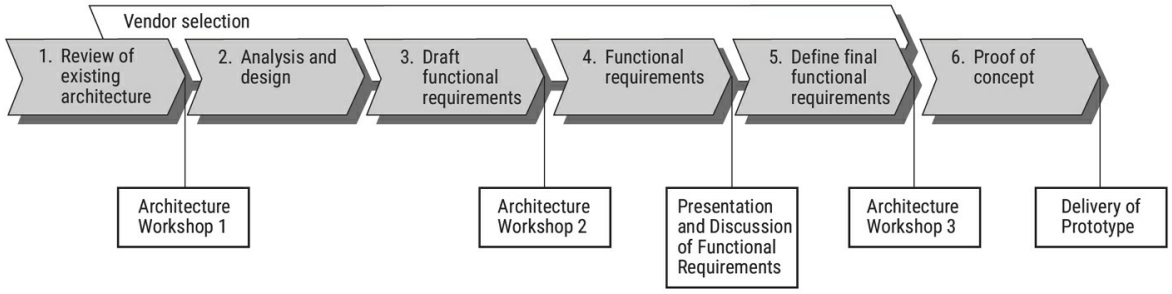
• Funding and costing model

• Data and algorithm

Related implementation projects that prepare for deployment should also be part of the POC because they will be used in the same way as they are used in the production physical architecture. At the end of this phase, a last workshop is

held where the production sizing and layout is adapted to include POC conclusions.

Figure 3.12—Project Phases of Physical Architecture Analysis



Additional considerations may apply if the entity goes in for an outsourcing/offshoring model for deployment and operation of applications.

Also, the platform for operation of the IT environment (i.e., owned, cloud-based, virtualization) can give rise to additional considerations. For example, if the enterprise operates in a highly regulated industry or an industry that demands high levels of availability, adequate redundancy and safeguards for ensuring data privacy and confidentiality may have to be factored in while testing the POC.

Planning Implementation of Infrastructure

To ensure the quality of the results, it is necessary to use a phased approach to fit the entire puzzle together. It is also fundamental to set up the communication processes to other projects like those described earlier.

Through these different phases the components are fit together, and a clear understanding of the available and contactable vendors is established by using the selection process during the procurement phase and beyond.

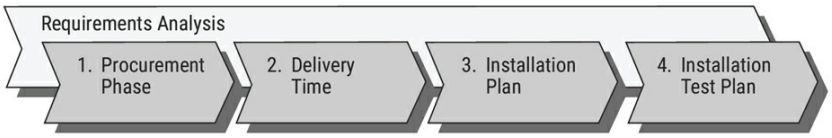
Furthermore, it is necessary to select the scope of key business and technical requirements to prepare the next steps, which include the development of the delivery, installation and test plans. Moreover, to ensure a future proven solution, it is crucial to choose the right partners with the right skills.

As shown in **figure 3.13,** the requirements analysis is not part of this process but constantly feeds results into the process. If a Gantt chart is produced with these

phases, most likely some phases overlap; therefore, the different phases must be considered an iterative process.

During the four different phases, it is necessary to fit all the components

Figure 3.13—Project Phases of Planning the Implementation of Infrastructure



together to prepare for projects downstream (e.g., data migration).

Procurement Phase

During the procurement phase, communication between the business and the analysis project is established to provide an overview of the chosen solution and determine the quantity structure of the deliverables. The requirements statements are also produced. Additionally, the procurement process begins the service-level management process. During these activities, the preferred partners are invited to the negotiations process and the deliverables, contracts and SLAs are signed (**figure 3.14**).

Delivery Time

During the delivery time phase, the delivery plan is developed (**figure 3.15**).

This phase overlaps in some parts with the procurement phase.

The delivery plan should include topics such as priorities, goals and nongoals, key facts, principles, communication strategies, key indicators, and progress on key tasks and responsibilities.

Installation Plan

During the installation planning phase, the installation plan is developed in cooperation with all affected parties (**figure 3.16**).

An additional step is to review the plan with the involved parties and, of course, with those responsible for the integration projects. This is an iterative process.

Figure 3.14—Procurement Phases

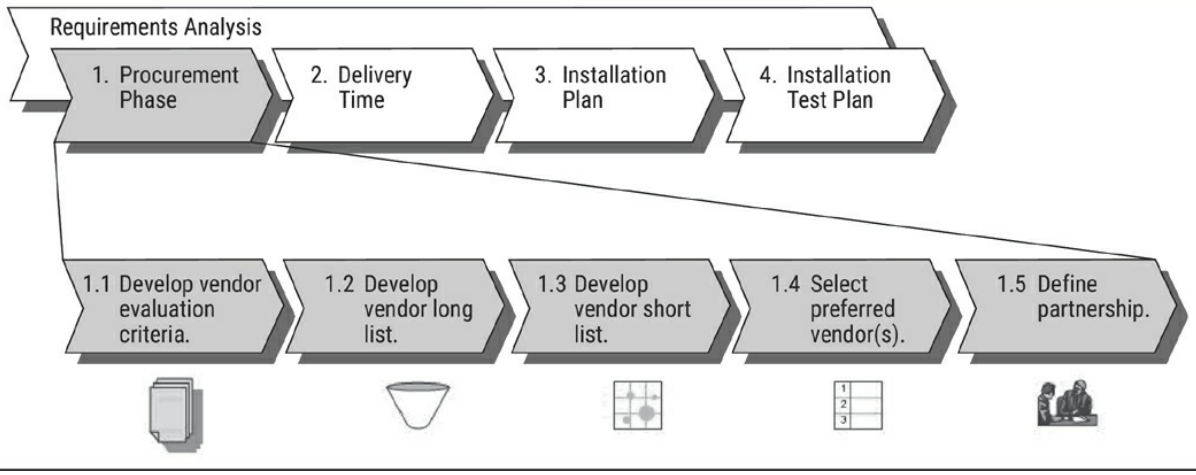


Figure 3.15—Delivery Time

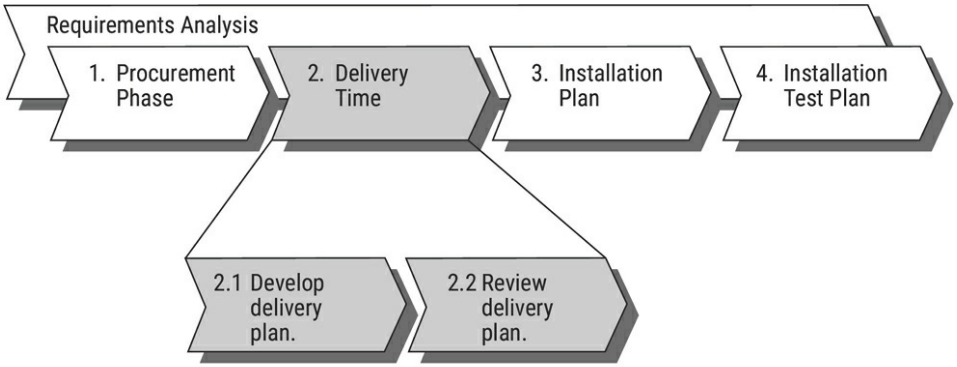
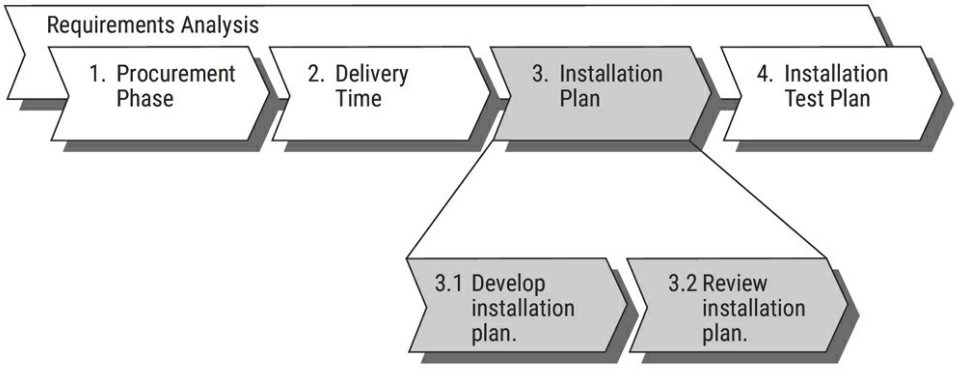


Figure 3.16—Installation Plan



Installation Test Plan

Based on the known dependencies of the installation plan, the test plan is developed (**figure 3.16**).

The test plan includes test cases, basic requirements' specifications, definition of the processes, and, as far as possible, measurement information for the applications and the infrastructure. Part one of the project (analysis of the physical architecture) must be completed, and the needed infrastructure decisions must be made.

3.3.8 HARDWARE/SOFTWARE ACQUISITION

Selection of a computer hardware and software environment frequently requires the preparation of specifications for distribution to

hardware/software (HW/SW) vendors and criteria for evaluating vendor proposals. The specifications are sometimes presented to vendors in the form of an invitation to tender (ITT), also known as a request for proposal (RFP).

The specifications must define, as completely as possible, the usage, tasks and requirements for the equipment needed and must include a description of the environment in which that equipment will be used.

When acquiring a system, the specifications should include the following:

• Organizational descriptions indicating whether the computer facilities are centralized or decentralized, distributed, outsourced, manned or lights-out

• HW/SW evaluation assurance levels (EALs) for security robustness

• Information processing requirements such as:

– Major existing application systems and future application systems

– Workload and performance requirements

– Processing approaches (e.g., online/batch, client-server, real-time databases, continuous operation)

• Hardware requirements such as:

– CPU speed

– Disk space requirements

– Memory requirements

– Number of CPUs required

– Peripheral devices (e.g., sequential devices such as tape drives; direct access devices such as magnetic disk drives, printers, compact disc drives, digital video disc drives, universal serial bus [USB] peripherals and secure digital multimedia cards [SD/MMC]) required or to be

excluded (usually for security reasons)

– Data preparation/input devices that accept and convert data for machine processing

– Direct entry devices (e.g., terminals, point-of-sale terminals or automated teller machines)

– Networking capability (e.g., Ethernet connections, modems and

integrated services digital network [ISDN] connections)

– Number of terminals or nodes the system needs to support

• System software applications such as:

– OS software (current version and any required upgrades)

– Utilities

– Compilers

– Program library software

– Database management software and programs

– Communications software

– Access control software

– Job scheduling software

• Support requirements such as:

– System maintenance (for preventive, detective [fault reporting] or corrective purposes)

– Training (user and technical staff)

– Backups (daily and disaster backups)

– Patching

• Adaptability requirements such as:

– Hardware and software upgrade capabilities

– Compatibility with existing hardware and software platforms

– Changeover to other equipment capabilities

• Constraints such as:

– Staffing levels

– Existing hardware capacity

– Delivery dates

• Conversion requirements such as:

– Test time for the hardware and software

– System conversion facilities

– Cost/pricing schedule

Acquisition Steps

When purchasing (acquiring) HW/SW from a vendor, consideration should be given to the following:

• Testimonials or visits with other users

• Provisions for competitive bidding

• Analysis of bids against requirements

• Comparison of bids against each other using predefined evaluation criteria

• Analysis of the vendor’s financial condition

• Analysis of the vendor’s capability to provide maintenance and support (including training)

• Review of delivery schedules against requirements

• Pedigree of the hardware to verify it is not sourced from “gray market”

supply sources (through distribution sources that are legal but are unofficial, unauthorized or unintended by the original manufacturer) that can increase the risk of malware and other unknown operability of the product

• Analysis of hardware and software upgrade capability

• Analysis of security and control facilities

• Evaluation of performance against requirements

• Review and negotiation of price

• Review of contract terms (including warranties, penalties and right-to-audit clauses)

• Preparation of a formal written report summarizing the analysis for each of the alternatives and justifying the selection based on benefits and cost The criteria and data used for evaluating vendor proposals should be properly planned and documented. The following are some of the criteria that should be considered in the evaluation process:

• **Turnaround time**—The time that the help desk or vendor takes to fix a problem from the moment it is logged in

• **Response time**—The time a system takes to respond to a specific query by the user

• **System reaction time**—The time taken for logging into a system or getting connected to a network

• **Throughput**—The quantity of useful work made by the system per unit of time. Throughput can be measured in instructions per second or some other unit of performance. When referring to a data transfer operation,

throughput measures the useful data transfer rate and is expressed in kilobits per second (Kbps), megabits per second (Mbps) and gigabits per second (Gbps).

• **Workload**—The capacity to handle the required volume of work or the volume of work that the vendor's system can handle in a given time frame

• **Compatibility**—The capability of an existing application to run successfully on the newer system supplied by the vendor

• **Capacity**—The capability of the newer system to handle a number of simultaneous requests from the network for the application and the volume of data that it can handle from each of the users

• **Utilization**—The system availability time versus the system downtime **IS Auditor's Role in Hardware Acquisition**

When performing an audit of this area, an IS auditor should:

• Determine if the acquisition process began with a business need and whether the hardware requirements for this need were considered in the specifications.

• Determine if several vendors were considered and whether the comparison between them was done according to the aforementioned criteria.

3.3.9 SYSTEM SOFTWARE ACQUISITION

Every time a technological development has allowed for increased computing speeds or new capabilities, these have been absorbed immediately by the demands placed on computing resources by more ambitious applications.

Consequently, improvements have led to decentralized, interconnected open systems through functions bundled in OS software to meet these needs. For example, network management and connectivity are features now found in most

OSs.

It is IS management's responsibility to be aware of HW/SW capabilities because they may improve business processes and provide expanded application services to businesses and customers in a more effective way.

Short- and long-term plans should document IS management's plan for migrating to newer, more efficient and more effective OSs and related systems software.

When selecting new system software, a number of business and technical issues must be considered including:

• Business, functional and technical needs and specifications

• Cost and benefit(s)

• Obsolescence

• Compatibility with existing systems

• Security

• Demands on existing staff

• Training and hiring requirements

• Future growth needs

• Impact on system and network performance

• Open source code versus proprietary code

The feasibility study should contain documentation that supports the decision to acquire the software. Depending on the software required there could be four cases:

1. Software is required for a generic business process for which vendors are available and software can be implemented without customization.

2. Software (the vendor's) needs to be customized to suit business processes.

3. Software needs to be developed by the vendor.

4. Software is available as a service through the cloud (software as a service

[SaaS]). This is generally available for generic processes.

A project team with participation by technical support staff and key users should be created to write an RFP or ITT. An RFP needs to be prepared separately for each case mentioned previously. The invitation to respond to an RFP should be widely distributed to appropriate vendors and, if possible, posted via a public procurement medium (Internet or newspaper). This process allows the business to determine which of the responding vendors'

products offers the best solution at the most cost-effective price.

The RFP should include the areas shown in **figure 3.17**.

When the product and related services are known in advance, a user organization often prefers an ITT so it can obtain the best combination of price and services. This is more applicable when procurement of hardware,

network, database, etc., is involved. When the requirement is more toward a solution and related support and maintenance, an organization generally prefers an RFP, so the capability, experience and approach can be measured against the requirement. This is more applicable in system integration projects such as ERP and supply chain management (SCM) that involve delivery or escrowing of source code.

Figure 3.17—RFP Contents

Item	**Description**
Product versus system	The chosen vendor's product should come as close as possible to
requirements	

meeting the defined requirements of the system. If no vendor's

product meets all of the defined requirements, the project team, especially the users, will have to decide whether to accept the

deficiencies. An alternative to living with a product's deficiencies is for the vendor or the purchaser to make customized changes to the product.

Product scalability and

The project management should not only look at vendor's product

interoperability

ability to meet the existing requirements for the project but also the ability of the product to grow and/or contract with the organization's business processes. Vendor products should be assessed as to the applications' ability to interconnect with other systems whose

interconnections are currently out of the project's scope but may be needed in the future.

Customer references

Project management should check vendor-supplied references to

validate the vendor's claims of product performance and completion of work by the vendor.

Vendor viability/financial

The vendor supplying or supporting the product should be reputable stability

and able to provide evidence of financial stability. A vendor may not be able to prove financial stability; if the product is new, the vendor presents a substantially higher risk to the organization.

Availability of complete and

The vendor should be willing and able to provide a complete set of reliable documentation

system documentation for review prior to acquisition. The level of detail and precision found in the documentation may be an indicator of the detail and precision utilized within the design and

programming of the system itself.

Vendor support

The vendor should have available a complete line of support products for the software package. This may include a 24-hour, seven-day-a-week help line, onsite training during implementation, product

upgrades, automatic new version notification and onsite maintenance, if requested.

Source code availability

The source code should be received either from the vendor initially or there should be provisions for acquiring the source code in the event that the vendor goes out of business. Usually, these clauses are part of a software escrow agreement in which a third party holds the software in escrow should such an event occur. The acquiring company should ensure that product updates and program fixes are included in the escrow agreement.

Number of years of

More years indicate stability and familiarity with the business that the experience in offering the

product supports.

product

A list of recent or planned

A short list suggests the product is not being kept current.

enhancements to the

product, with dates

Number of client sites using

A larger number suggests wide acceptance of the product in the

the product with a list of

marketplace.

current users

Acceptance testing of the

Such testing is crucial in determining whether the product really product

satisfies the system requirements. This is allowed before a purchasing commitment must be made.

Often, prior to the development of an RFP, an organization will develop a request for information (RFI) to solicit software development vendors for advice in addressing problems with existing systems. Information obtained in this manner may be used to develop an RFP. The project team needs to carefully examine and compare the vendors' responses to the RFP. This comparison should be done using an objective method such as a scoring and ranking methodology. After the RFP responses have been examined, the project team may be able to identify a single vendor whose product satisfies most or all of the stated requirements in the RFP. Other times, the team may narrow the list to two or three acceptable candidates (i.e., short list of vendors). In evaluating the best-fit solution and vendor against the given set of business requirements and conditions, a suitable methodology of evaluation should be adopted. The methodology should ensure objective, equitable and fair comparison of the products/vendors (e.g., a gap analysis to find out the differences between requirements and software, the parameters required to modify).

It is important to keep in mind the minimum and recommended requirements to use software, including:

• Required hardware such as memory, disk space, and server or client characteristics

• OS versions and patch levels supported

• Additional tools such as import and export tools

• Databases supported

In addition, it is likely that more than one product/vendor fits the requirements, with advantages and disadvantages with respect to each other.

To resolve such a situation, agenda-based presentations should be requested from the short-listed vendors. The agenda-based presentations are scripted business scenarios that are designed to show how the vendor will perform certain critical business functions. Vendors are typically invited to demonstrate their product and follow the sample business scenarios given to them to prepare. It is highly recommended to include adequate participation from various user groups when evaluating the product's/vendor's fit and the system's ease of use. The project team thus has an opportunity to check the intangible issues such as the vendor's knowledge of the product and the vendor's ability to understand the business issue at hand. Having each short-listed vendor demonstrate its product following a scripted document also enables the project team to evaluate and finalize the product/vendor selection with knowledge and objectivity built into the process. The finalist vendor candidate is then requested to organize site visits to confirm the findings from the agenda-based presentations and check the system in a live environment.

Once the finalist is confirmed, a conference room pilot needs to be conducted. A conference room pilot enables the project team to understand the system with a hands-on session with business end users and identify the areas that need certain customizations or workarounds.

Additionally, for the short list of vendors, it can be beneficial for the project team to talk to current users of each of the potential products. If it can be arranged and cost-justified, an onsite visit can be even more beneficial.

Whenever possible, the organizations chosen should be those that use the products in a manner that is similar to the way the organization selecting the products plans to use them.

An IS auditor should encourage the project team to contact current users. The

information obtained from these discussions or visits validates statements made in the vendor's proposal and can determine which vendor is selected.

The discussions with the current users should concentrate on each vendor's:

• **Reliability**—Are the vendor's deliverables (enhancements or fixes) dependable?

• **Commitment to service**—Is the vendor responsive to problems with its product? Does the vendor deliver on time?

• **Commitment to providing training, technical support and**

documentation for its product—What is the level of customer satisfaction?

Upon completing the activities cited, vendor presentations and final evaluations, the project team can make a product/vendor selection. The reasons for making a particular choice should be documented.

The last step in the acquisition process is to negotiate and sign a contract for the chosen product. Appropriate legal counsel should review the contract prior to its signing. The contract should contain the following items:

• Specific description of deliverables and their costs

• Commitment dates for deliverables

• Commitments for delivery of documentation, fixes, upgrades, new release notifications and training

• Commitments for data migration

• Allowance for a software escrow agreement, if the deliverables do not include source code

• Description of the support to be provided during installation/customization

• Criteria for user acceptance

• Provision for a reasonable acceptance testing period, before the commitment to purchase is made

• Allowance for changes to be made by the purchasing company

• Maintenance agreement

• Allowance for copying software for use in business continuity efforts and for test purposes

• Payment schedule linked to actual delivery dates

• Confidentiality clauses

• Data protection clauses

Managing the contract should also involve a major level of effort to ensure that deployment efforts are controlled, measured and improved on, where appropriate. This may include regular status reporting requirements.

Additionally, the milestones and metrics to be reported against should be agreed with the vendor.

Integrated Resource Management Systems

An integrated solutions implementation is a very large software acquisition project. The acquisition and implementation of an ERP system impacts the way that an organization does business and its entire control environment, technological direction and internal resources. Generally, an organization that adopts an integrated solution is required to convert management

philosophies, policies and practices to those of the integrated software solution providers, notwithstanding the numerous customization options. In this respect, such a solution will either impair or enhance IT’s ability to support the organization’s mission and goals. When considering a change of this magnitude, it is imperative that a thorough impact and risk assessment be conducted.

When implementing an ERP solution or any off-the-shelf software, the business unit has the option of implementing and configuring the new system in the simplest configuration possible: as-is, out-of-the-box, and not developing any additional functionality or customization to bridge the gaps in an organization’s specific business processes. The business opts to change business processes to suit the industry standard as dictated by the software solution.

While this decision results in less software design, development and testing work

than does customization, it does require greater change in the business units to work differently. Due to the large costs in software development, maintenance, and continuous upgrading and patching, customization is not usually recommended by software vendors.

Because of the magnitude of the risk involved, it is imperative that senior management assess and approve all plans and changes in the system's architecture, technological direction, migration strategies and IS budgets.

IS Auditor's Role in Software Acquisition

An IS auditor should be involved in the software acquisition process to determine whether an adequate level of security controls has been considered prior to any agreement being reached. If security controls are not part of the software, it may become difficult to ensure data integrity for the information that will be processed through the system. Risk involved with the software package includes inadequate audit trails, password controls and overall security of the application. Because of the risk, an IS auditor should ensure that these controls are built into the software application.

An IS auditor should perform the following when reviewing software acquisition:

• Analyze the documentation from the feasibility study to determine whether the decision to acquire a solution was appropriate (including consideration of common criteria evaluations).

• Review the RFP to ensure that it covers the items listed in this section.

• Determine whether the selected vendor is supported by RFP

documentation.

• Attend agenda-based presentations and conference room pilots to ensure that the system matches the vendor's response to the RFP.

• Review the vendor contract prior to its signing to ensure that it includes the items listed.

• Ensure the contract is reviewed by legal counsel before it is signed.

• Review the RFP to ensure security responses are included by the vendor.

3.4 CONTROL IDENTIFICATION AND DESIGN

An IS auditor must be able to identify and understand controls designed to ensure the authorization, accuracy and completeness of data input to, processing by and output from various business and computer applications.

An IS auditor must also be familiar with control techniques and how each may be evidenced in the form of reports, logs and audit trails.

3.4.1 INPUT/ORIGINATION CONTROLS

Input control procedures must ensure that every transaction to be processed is

entered, processed and recorded accurately and completely. These controls should ensure that only valid and authorized information is input and these transactions are processed only once. These include machine and manual inputs. In an integrated systems environment, output generated by one system is the input for another system. Therefore, the system receiving the output of another system as input/origination must, in turn, apply edit checks, validations and access controls to those data.

Input Authorization

Input authorization verifies that all transactions have been authorized and approved by management. Authorization of input helps ensure that only authorized data are entered for processing by applications. Authorization can be performed online when the data are entered into the system. A computer-generated report listing the items requiring manual authorization may also be generated. It is important that controls exist throughout processing to ensure that the authorized data remain unchanged. This can be accomplished through various accuracy and completeness checks incorporated into an application's design.

Types of authorization include:

• **Signatures on batch forms or source documents**—Provide evidence of proper authorization

• **Online access controls**—Ensure that only authorized individuals may access data or perform sensitive functions

• **Unique passwords**—Ensure that access authorization cannot be compromised through use of another individual's authorized data access.

Individual unique passwords also provide accountability for data changes.

• **Terminal or client workstation identification**—Limits input to specific terminals or workstations as well as to individuals. Terminals or client workstations in a network can be configured with a unique form of identification such as serial number or computer name that is authenticated by the system.

• **Source documents**—Record the data. A source document may be a piece of paper, a turnaround document or an image displayed for online data input. A well-designed source document achieves several purposes. It increases the speed and accuracy with which data can be recorded, controls

work flow, facilitates preparation of the data in machine-readable form for pattern recognition devices, increases the speed and accuracy with which data can be read, and facilitates subsequent reference checking.

• **Input data validation**—Ensures that information is being received in the expected format and that there is no malicious or manipulative activity taking place with inputs

Ideally, source documents should be preprinted or electronic forms to provide consistency, accuracy and legibility. Source documents should include standard headings, titles, notes and instructions. Source document layouts should:

• Emphasize ease of use and readability.

• Group similar fields together to facilitate input.

• Provide predetermined input codes to reduce errors.

• Contain appropriate cross-reference numbers or a comparable identifier to facilitate research and tracing.

• Use boxes to prevent field size errors.

• Include an appropriate area for management to document authorization.

All source documents should be appropriately controlled. Procedures should be established to ensure that all source documents have been input and considered. Prenumbering source documents facilitates this control.

Batch Controls and Balancing

Batch controls group input transactions to provide control totals. The batch control can be based on total monetary amount, total items, total documents or hash totals:

• **Total monetary amount**—Verification that the total monetary value of items processed equals the total monetary value of the batch documents.

For example, the total monetary value of the sales invoices in the batch agrees with the total monetary value of the sales invoices processed. This provides assurance on the completeness and accuracy of the sales value processed for the batch.

• **Total items**—Verification that the total number of items included on each document in the batch agrees with the total number of items processed. For example, the total number of units ordered in the batch of invoices agrees

with the total number of units processed. This provides assurance on the completeness and accuracy of the units ordered in the batch processed.

• **Total documents**—Verification that the total number of documents in the batch equals the total number of documents processed. For example, the total number of invoices in a batch agrees with the total number of invoices processed. This provides assurance on the completeness of the number of invoices processed.

• **Hash totals**—Verification that the total in a batch agrees with the total calculated by the system. Hash total is the total of nonvalue numeric fields in the batch (such as total of dates or customer number fields, which, by themselves, do not have informative value). This provides assurance on the completeness and accuracy of data entered for the numeric fields in the batch.

Batch header forms are a data preparation control. All input forms should be clearly identified with the application name and transaction codes. Batch

balancing can be performed through manual or automated reconciliation.

Batch totaling must be combined with adequate follow-up procedures.

Adequate controls should exist to ensure that each transaction creates an input document, all documents are included in a batch, all batches are submitted for processing, all batches are accepted by the computer, batch reconciliation is performed, procedures for the investigation and timely correction of differences are followed, and controls exist over the resubmission of rejected items.

Types of batch balancing include:

• **Batch registers**—Enable recording of batch totals and subsequent comparison with system reported totals

• **Control accounts**—Control account use through an initial edit file to determine batch totals. The data are then processed to the master file, and a reconciliation is performed between the totals processed during the initial edit file and the master file.

• **Computer agreement**—Compares batch header details that record the batch totals to calculated totals, either accepting or rejecting the batch **Error Reporting and Handling**

Input processing requires that controls be identified to verify that only correct data are accepted into the system and input errors are recognized and corrected.

Data conversion error corrections are needed during the data conversion process. Errors can occur due to duplication of transactions and inaccurate data entry. These errors can, in turn, impact the completeness and accuracy of the data. Corrections to data should be processed through normal data conversion processes and should be verified, authorized and reentered into the system as a part of the normal processing.

Input error handling can be processed by:

• **Rejecting only transactions with errors**—Only transactions containing errors would be rejected; the rest of the batch would be processed.

• **Rejecting the whole batch of transactions**—Any batch containing errors

would be rejected for correction prior to processing.

• **Holding the batch in suspense**—Any batch containing errors would not be rejected; however, the batch would be held in suspense, pending correction.

• **Accepting the batch and flagging error transactions**—Any batch containing errors would be processed; however, those transactions containing errors would be flagged for identification, enabling subsequent error correction.

Input control techniques:

• **Transaction log**—Contains a detailed list of all updates. The log can be either manually maintained or provided through automatic computer logging. A transaction log can be reconciled to the number of source documents received to verify that all transactions have been input.

• **Reconciliation of data**—Controls whether all data received are properly recorded and processed

• **Documentation**—Records (written evidence) user, data entry and data control procedures

• **Error correction procedures**—Includes:

– Logging of errors

– Timely corrections

– Upstream resubmission

– Approval of corrections

– Suspense file

– Error file

– Validity of corrections

• **Anticipation**—Anticipates (user or control group) the receipt of data

• **Transmittal log**—Documents transmission or receipt of data

• **Cancellation of source documents**—Procedures to cancel source documents such as by punching with holes or marking them to avoid duplicate entry

• **Input sanitization**—Checks user input prior to storing it in a database or using it for other purposes in order to prevent malicious code injection **3.4.2 PROCESSING PROCEDURES AND CONTROLS**

Processing procedures and controls are meant to ensure the reliability of application program processing. An IS auditor should understand the procedures and controls that can be exercised over processing to evaluate what exposures are covered by these controls and what exposures remain.

Data Validation and Editing Procedures

Procedures should be established to ensure that input data are validated and edited as close to the time and point of origination as possible.

Preprogrammed input formats ensure that data are input to the correct field in the correct format. If input procedures allow supervisor overrides of data validation and editing, automatic logging should occur. A manager who did not initiate the override should review this log. Data validation is meant to identify data errors, incomplete or missing data, and inconsistencies among related data items. Front-end data editing and validation can be performed if intelligent terminals are used.

Edit controls are preventive controls that are used in a program before data are processed. If not in place or not working effectively, the preventive controls are not effective. This may cause processing of inaccurate data.

Figure 3.18 describes various types of data validation edits.

Processing Controls

Processing controls are meant to ensure the completeness and accuracy of accumulated data. They ensure that data in a file/database remain complete and accurate until changed as a result of authorized processing or modification routines. The following are processing control techniques that can be used to address the issues of completeness and accuracy of accumulated data:

Figure 3.18—Data Validation Edits and Controls

Edits

Description

Sequence check

The control number follows sequentially and any sequence or

duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoices begin with 12001 and end with

15045. If any invoice larger than 15045 is encountered during

processing, that invoice would be rejected as an invalid invoice number.

Limit check

Data should not exceed a predetermined amount. For example,

payroll checks should not exceed US $4,000. If a check exceeds US

$4,000, the data would be rejected for further

verification/authorization.

Range check

Data should be within a predetermined range of values. For example, product type codes range from 100 to 250. Any code outside this

range should be rejected as an invalid product type.

Validity check

Programmed checking of the data validity in accordance with

predetermined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, the record should be rejected.

Reasonableness check

Input data are matched to predetermined reasonable limits or

occurrence rates. For example, a widget manufacturer usually

receives orders for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table lookups

Input data comply with predetermined criteria maintained in a

computerized table of possible values. For example, the input clerk enters a city code of 1 to 10. This number corresponds with a

computerized table that matches the code to a city name.

Existence check

Data are entered correctly and agree with valid predetermined

criteria. For example, a valid transaction code must be entered in the transaction code field.

Key verification

The keying process is repeated by a separate individual using a

machine that compares the original keystrokes to the repeated keyed input. For example, the worker number is keyed twice and compared to verify the keying process.

Check digit

A numeric value that has been calculated mathematically is added to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted. This control is effective in detecting transposition and transcription errors. For example, a check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check

A field should always contain data rather than zeros or blanks. A check of each byte of that field should be performed to determine that some form of data, not blanks or zeros, is present. For example, a worker number on a new employee record is left blank. This is

identified as a key field and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check

New transactions are matched to those previously input to ensure that they have not already been entered. For example, a vendor invoice number agrees with previously recorded invoices to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Logical relationship check

If a particular condition is true, then one or more additional

conditions or data input relationships may be required to be true and consider the input valid. For example, the hire date of an employee may be required to be more than 16 years past his/her date of birth.

• **Manual recalculations**—Manually recalculation of a sample of transactions to ensure that processing is accomplishing the anticipated task

• **Editing**—A program instruction or subroutine that tests the accuracy, completeness and validity of data. It may be used to control input or later processing of data.

• **Run-to-run totals**—Verification of data values through the stages of application processing. Run-to-run total verification ensures that data read into the computer were accepted and then applied to the updating process.

• **Programmed controls**—Software that detects and initiates corrective action for errors in data and processing. For example, if the incorrect file or file version is provided for processing, the application program could display messages instructing that the proper file and version be used.

• **Reasonableness verification of calculated amounts**—An application

program that verifies the reasonableness of calculated amounts. The reasonableness can be tested to ensure appropriateness to predetermined criteria. Any transaction that is determined to be unreasonable may be rejected pending further review.

• **Limit checks on amounts**—Assurance provided, through the use of predetermined limits, that amounts have been keyed or calculated correctly.

Any transaction exceeding the limit may be rejected for further

investigation.

• **Reconciliation of file totals**—Should be performed on a routine basis.

Reconciliations may be performed through the use of a manually

maintained account, a file control record or an independent control file.

• **Exception reports**—Generated by a program that identifies transactions or data that appear to be incorrect. These items may be outside a

predetermined range or may not conform to specified criteria.

Data File Control Procedures

File controls should ensure that only authorized processing occurs to stored data. Types of controls over data files are shown in **figure 3.19**. Contents of data files, or database tables, generally fall into four categories:

• **System control parameters**—The entries in these files change the workings of the system and may alter controls exercised by the system—

for example, the tolerance allowed before an exceptional transaction is reported or blocked. Any change to these files should be controlled in a similar way to program changes.

• **Standing data**—These “master files” include data, such as supplier/customer names and addresses, that do not frequently change and are referred to during

processing. These data should be authorized before entry or maintenance. Input controls may include a report of changed data that is checked and approved. Audit trails may log all changes.

• **Master data/balance data**—Running balances and totals that are updated by transactions should not be capable of adjustment except under strict approval and review controls. Audit trails are important here since there may be financial reporting implications for the change.

• **Transaction files**—These are controlled using validation checks, control totals, exception reports, etc.

It should be noted that the controls built into an application represent the management design of controls on how a business process should be run.

While an application contains the rules for the business, the data that are the outcome of the processing are stored in the database. An entity may have the best controls built into the application, but if management personnel directly update data in the database, then the benefit of the best controls in the application will be overridden.

However, in some situations, organizations may have to carry out direct updates to a database. For example, if, due to a systems outage, the transactions could not be processed in real time for a few days, it is not practical to insist that once the system availability is restored, the backlog should be entered through the application (front end) before the transactions of the subsequent days are entered or processed. In such cases, management may decide to catch up on the backlog by directly updating the transactions in the database (back end).

An IS auditor should ensure that there are controls in place to ensure that such direct back-end data fixes are supported by authorization of the business for completeness and accuracy and are processed subject to computer operations controls. The important point to remember is that, in any organization, the quality of application controls is only as good as the quality of controls around direct back-end data fixes.

3.4.3 OUTPUT CONTROLS

Output controls provide assurance that the data delivered to users will be presented, formatted and delivered in a consistent and secure manner.

Output controls include:

• **Logging and storage of negotiable, sensitive and critical forms in a secure place**—Negotiable, sensitive or critical forms should be properly logged and secured to provide adequate safeguards against theft, damage or disclosure. The form log should be routinely reconciled to have inventory on hand, and any discrepancies should be properly researched.

• **Computer generation of negotiable instruments, forms and signatures**

—The computer generation of negotiable instruments, forms and signatures

should be properly controlled. A detailed listing of generated forms should be compared to the physical forms received. One should properly account for all exceptions, rejections and mutilations.

• **Report accuracy, completeness and timeliness**—Often reports are generated using third-party data analysis and reporting applications (ESSbase, etc.). Even with the most reliable and accurate data sources, improperly configured, constructed and prepared reports are still a significant risk. Report design and generation specifications, templates and creation/change request processes are critical system output controls.

• **Reports generated from the system**—These represent the data that management relies upon for business decisions and review of business results. Therefore, ensuring the integrity of data in reports is key for the reliability of information in information systems. An IS auditor should validate that the reports are accurate and provide correct representation of the source data.

Figure 3.19—Data File Controls

Method

Description

Before and after image

Computer data in a file prior to and after a transaction is processed reporting

can be recorded and reported. The before and after images make it possible to

trace the impact transactions have on computer records.

Maintenance error reporting

Control procedures should be in place to ensure that all error reports and handling

are properly reconciled and corrections are submitted on a timely basis. To ensure SoD, error corrections should be reviewed properly and authorized by personnel who did not initiate the transaction.

Source documentation

Source documentation should be retained for an adequate time period retention

to enable retrieval, reconstruction or verification of data. Policies regarding the retention of source documentation should be enforced.

Originating departments should maintain copies of source

documentation and ensure that only authorized personnel have access.

When appropriate, source documentation should be destroyed in a

secure, controlled environment.

Internal and external

Internal and external labeling of removable storage media is

labeling

imperative to ensure that the proper data are loaded for processing.

External labels provide the basic level of assurance that the correct data medium is loaded for processing. Internal labels, including file header records, provide assurance that the proper data files are used and allow for automated checking.

Version usage

It is critical that the proper version of a file be used as well as the correct file, for

processing to be correct. For example, transactions should be applied to the most current database, while restart

procedures should use earlier versions.

Data file security

Data file security controls prevent unauthorized access by

unauthorized users that may have access to the application to alter data files. These controls do not provide assurances relating to the validity of data but ensure that unauthorized users who may have access to the application cannot alter stored data improperly.

One-for-one checking

Individual documents agree with a detailed listing of documents

processed by the computer. It is necessary to ensure that all

documents have been received for processing.

Prerecorded input

Certain information fields are preprinted on blank input forms to reduce initial input errors.

Transaction logs

All transaction input activity is recorded by the computer. A detailed listing, including date of input, time of input, user ID and terminal location, can then be generated to provide an audit trail. It also permits operations personnel to determine which transactions have been posted. This will help to decrease the research time needed to investigate exceptions and decrease recovery time if a system failure occurs.

File updating and

Proper authorization for file updating and maintenance is necessary to maintenance authorization

ensure that stored data are safeguarded adequately, correct and up to date. Application programs may contain access restrictions in

addition to the overall system access restrictions. The additional security may provide levels of authorization as well as an audit trail of file maintenance.

Parity checking

Data transfers in a computer system are expected to be made in a relatively error-free environment. However, when programs or vital data are transmitted, additional controls are needed. Transmission errors are controlled primarily by error-detecting or correcting codes.

The former is used more often because error-correcting codes are costly to implement and are unable to correct all errors. Generally, error detection methods such as a check bit and redundant

transmission are adequate. Redundancy checking is a common error-detection routine. A transmitted block of data containing one or more records or messages is checked for the number of characters or

patterns of bits contained in it. If the numbers or patterns do not conform to predetermined parameters, the receiving device ignores the transmitted data and instructs the user to retransmit. Check bits are often added to the transmitted data by the telecommunications control unit and may be applied either horizontally or vertically.

These checks are similar to the parity checks normally applied to data characters within on-premises equipment. A parity check on a single character generally is referred to as a vertical or column check, and a

parity check on all the equivalent bits is known as a horizontal, longitudinal or row check. Use of both checks greatly improves the possibilities of detecting a transmission error, which may be missed when either of those checks is used alone.

An IS auditor needs to apply an assessment approach in validating reports depending on the situation (more evaluation is required when the organization has undergone a system change or when evaluating customized reports against standard reports of a widely used application). Methods to validate reports

include the following:

• **Report distribution**—Output reports should be distributed according to authorized distribution parameters. Operations personnel should verify that reports are complete and delivered according to schedule. All reports should be logged prior to distribution. In most environments, processing output is spooled to a buffer or print spool on completion of job processing, where it waits for an available printer. Controls over access to the print spools are important to prevent reports from being deleted accidentally from print spools or directed to a different printer. In addition, changes to the output print priority can delay printing of critical jobs. Access to distributed reports can compromise confidentiality; therefore, physical distribution of reports should be controlled adequately. Reports containing sensitive data should be printed under secure, controlled conditions. Secure output drop-off points should be established. Output disposal should also be secured to ensure that no unauthorized access can occur. Electronic distribution should also be considered, and logical access controls should be put in place.

• **Balancing and reconciling**—Data processing application program output should be balanced routinely to the control totals. Audit trails should be provided to facilitate the tracking of transaction processing and the reconciliation of data.

• **Output error handling**—Procedures for reporting and controlling errors contained in the application program output should be established. The error report should be timely and delivered to the originating department for review and error correction.

• **Output report retention**—A record retention schedule should be adhered to firmly. Any governing legal regulations should be included in the retention policy.

• **Verification of receipt of reports**—To provide assurance that sensitive reports are properly distributed, the recipient should sign a log as evidence of receipt of output.

An IS auditor should be aware of existing concerns regarding record-retention policies for the organization and address legal requirements. Output can be restricted to particular IT resources or devices (e.g., a particular printer).

3.4.4 APPLICATION CONTROLS

Application controls are controls over the aforementioned input, processing and output functions. They include methods for ensuring that:

• Only complete, accurate and valid data are entered and updated in a computer system.

• Processing accomplishes the correct task.

• Processing results meet expectations.

• Data are maintained.

Application controls may consist of edit tests; totals; reconciliations; and identification and reporting of incorrect, missing or exception data.

Automated controls should be coupled with manual procedures to ensure proper investigation of exceptions.

These controls help ensure data accuracy, completeness, validity, verifiability and consistency, thus achieving data integrity and data reliability.

Implementation of these controls helps ensure that systems maintain integrity; applicable system functions operate as intended; and information contained by the system is relevant, reliable, secure and available when needed.

IS Auditor's Role in Reviewing Application Controls

When reviewing application controls, an IS auditor should perform the following activities:

• Identify the significant application components and the flow of transactions through the system and gain a detailed understanding of the application by reviewing the available documentation and interviewing appropriate

personnel.

• Identify the application control strengths and evaluate the impact of the control weaknesses.

• Develop a testing strategy.

• Test the controls to ensure their functionality and effectiveness by applying appropriate audit procedures.

• Evaluate the control environment by analyzing the test results and other audit evidence to determine that control objectives were achieved.

• Consider the operational aspects of the application to ensure its efficiency and effectiveness by comparing the system with efficient system design standards, analyzing procedures used and comparing them to

management's objectives for the system.

When auditing application controls, an IS auditor should:

• Plan the audit, set audit objectives and identify risk associated with the application being audited.

• Identify the significant application components and the flow of information through the system and gain a detailed understanding of the application by reviewing the available documentation and interviewing appropriate personnel. Developing a DFD can help visualize the flow of information.

Flow of Information Through the System

A transaction flowchart provides information regarding key application processing controls. Points where transactions are entered, processed and posted should be reviewed for control weaknesses. The IS auditor should consider the following:

• Understand and evaluate interfaces, including APIs, in case the application connects with other applications.

• Identify the application key control strengths and evaluate the impact of the control weaknesses to develop a testing strategy by analyzing the accumulated information.

• Review application system documentation to provide an understanding of the functionality of the application. In many cases, it is not feasible to review the whole application documentation. Thus, a selective review should be performed. Any changes to applications should be documented properly. To gain an

understanding of an application’s development, an IS

auditor should review the following documentation:

– **System development methodology documents**—Documents that describe the systems development approach used and include cost-benefit analysis and user requirements – **Functional design**

specifications—Documents that provide a detailed explanation of the application. An understanding of key control points should be noted during review of the design specifications.

– **Program changes**—Documents that detail any program change and provide evidence of authorization and a cross-reference to source code

– **User manuals**—Documents that provide the foundation for

understanding how the user is using the application. Often control weaknesses can be noted from the review of this document.

– **Technical reference documentation**—Documents that include vendor-supplied technical manuals for purchased applications in addition to any in-house documentation. Access rules and logic usually are included in these documents.

• Test the effectiveness of application controls. The best practice for testing involves multiple levels of testing. See section 3.5, Testing Methodologies, for more information.

• Report the results. The report should include the audit objectives, tests conducted, test results, and findings and recommendations.

Risk Assessment Model to Analyze Application Controls

Conducting a risk assessment provides information relating to the inherent risk of an application. This risk assessment model can be based on many factors, which may include a combination of the following:

• The quality of internal controls

• Economic conditions

• Recent accounting system changes

• Time elapsed since last audit

• Complexity of operations

• Changes in operations/environment

• Recent changes in key positions

• Time in existence

• Competitive environment

• Assets at risk

• Prior audit results

• Staff turnover

• Transaction volume

• Regulatory agency impact

• Monetary volume

• Sensitivity of transactions

• Impact of application failure

3.4.5 USER PROCEDURES

User procedures that should be observed and tested by an IS auditor include:

• **SoD**—Ensures that no individual has the capability of performing more than one of the following processes: origination, authorization, verification or distribution. Observation and review of job descriptions and review of authorization levels and procedures may provide information regarding the existence and enforcement of SoD.

• **Authorization of input**—Provides evidence of input authorization via written authorization on input documents or with the use of unique passwords. This can be tested by looking through a sampling of input documents for proper authorization or reviewing computer access rules.

Supervisor overrides of data validation and editing should be reviewed to ensure that automatic logging occurs. This override activity report should be tested for evidence of managerial review. Excessive overrides may indicate the need for modification of validation and editing routines to improve efficiency.

• **Balancing**—Verifies that run-to-run control totals and other application totals are reconciled on a timely basis. This may be tested by independent balancing or reviewing past reconciliations.

• **Error control and correction**—Provides evidence of appropriate review in the form of reports, research, timely correction and resubmission. Input errors and rejections should be reviewed prior to resubmission. Managerial review and authorization of corrections should be evidenced. Testing of this effort can be achieved by retabulating or reviewing past error corrections.

• **Distribution of reports**—Produces and maintains critical output reports in a secure area and distributes in an authorized manner. The distribution

process can be tested by observation and review of distribution output logs.

Access to online output reports should be restricted. Online access may be tested through a review of the access rules or by monitoring user output.

• **Review and testing of access authorizations and capabilities**—Provides information regarding access levels (control tables). Access should be based on job descriptions and should provide for SoD. Testing can be performed through the review of access rules to ensure that access has been granted as management intended.

• **Activity reports**—Provide details, by user, of activity volume and hours.

Activity reports should be reviewed to ensure that activity occurs only during authorized hours of operation.

• **Violation reports**—Record any unsuccessful and unauthorized access

attempts. Violation reports should indicate the terminal location, date and time of attempted access. These reports should evidence managerial review. Repeated unauthorized access violations may indicate attempts to circumvent access controls. Testing may include review of follow-up activities.

3.4.6 DECISION SUPPORT SYSTEM

A decision support system (DSS) is an interactive system that provides the user with easy access to decision models and data from a wide range of sources in order to support semistructured decision-making tasks typically for business purposes. It is an informational application that is designed to assist an organization in making decisions through data provided by business intelligence tools (in contrast to an operational application that collects the data in the course of normal business operations).

Typical information that a decision support application might gather and present would be:

• Comparative sales figures between one week and the next

• Projected revenue figures based on new product sales assumptions

• The consequences of different decision alternatives given past experience in the described context

A DSS may present information graphically and may include an expert system or AI. Further, it may be aimed at business executives or some other

group of knowledge workers.

Characteristics of a DSS include:

• It is aimed at solving less structured, underspecified problems that senior managers face.

• It combines the use of models or analytic techniques with traditional data access and retrieval functions.

• It emphasizes flexibility and adaptability to accommodate changes in the environment and the decision-making approach of the users.

A principle of DSS design is to concentrate less on efficiency (i.e., performing tasks quickly and reducing costs) and more on effectiveness (i.e., performing the right task). Therefore, DSSs are often developed using 4GL

tools that are less efficient but allow for flexible and easily modified systems.

A DSS is often developed with a specific decision or well-defined class of decisions to solve; therefore, some commercial software packages that claim to be a DSS are nothing more than a DSS generator (tools with which to construct a DSS).

Design and Development

Prototyping is the most popular approach to DSS design and development.

Prototyping usually bypasses the usual requirement definition. System requirements evolve through the user's learning process. The benefits of prototyping include the following:

• Learning is explicitly incorporated into the design process because of the iterative nature of the system design.

• Feedback from design iterations is rapid to maintain an effective learning process for the user.

• The user's expertise in the problem area helps the user suggest system improvements.

• The initial prototype must be inexpensive to create.

Implementation and Use

It is difficult to implement a DSS because of its discretionary nature. Using a DSS to solve a problem represents a change in behavior on the part of the user. Implementing a DSS is an exercise in changing an organization's

behavior. The main challenge is to get the users to accept the use of software.

The following are the steps involved in changing behavior:

• **Unfreezing**—This step alters the forces acting on individuals such that the individuals are distracted sufficiently to change. Unfreezing is accomplished either through increasing the pressure for change or by reducing some of the

threats of or resistance to change.

• **Moving**—This step presents a direction of change and the actual process of learning new attitudes.

• **Refreezing**—This step integrates the changed attitudes into the individual's personality.

Risk Factors

Developers should be prepared for eight implementation risk factors: 1. Nonexistent or unwilling users

2. Multiple users or implementers

3. Disappearing users, implementers or maintainers

4. Inability to specify purpose or usage patterns in advance

5. Inability to predict and cushion impact on all parties

6. Lack or loss of support

7. Lack of experience with similar systems

8. Technical problems and cost-effectiveness issues

Implementation Strategies

To plan for risk and prevent it from occurring:

• Divide the project into manageable pieces.

• Keep the solution simple.

• Develop a satisfactory support base.

• Meet user needs and institutionalize the system.

Assessment and Evaluation

The true test of a DSS lies in whether it improves a manager's decision-making, which is not easily measured. A DSS also rarely results in cost displacements such as a reduction in staff or other expenses. In addition, because a DSS is evolutionary in nature, it lacks neatly defined completion dates.

Using an incremental approach to DSS development reduces the need for evaluation. By developing one step at a time and achieving tangible results at the end of each step, the user does not need to make extensive commitments of time and money at the beginning of the development process.

The DSS designer and user should use broad evaluation criteria. These criteria should include:

• Traditional cost-benefit analysis

• Procedural changes, more alternatives examined and less time consumed in making the decision

• Evidence of improvement in decision-making

• Changes in the decision process

DSS Common Characteristics

DSSs share many common characteristics. These include:

• Oriented toward decision making

• Usually based on 4GL

• Surfable

• Linkable

• Drill-down

• Semaphores (signals to automatically alert when a decision needs to be made)

• Time series analysis

• What if (refers to scenario modeling, such as determining the end result of a

changing variable or variables)

• Sensitivity analysis

• Goal-seeking

• Excellent graphic presentations

• Dynamic graphic, data editing

• Simulation

PART B: INFORMATION SYSTEMS

IMPLEMENTATION

Information systems implementation is when the system is installed and moved into the production environment after appropriate system and users'

acceptance testing. This is the stage at which:

• End users are notified.

• Data entry or conversions occur.

• Training takes place.

• Post-implementation reviews occur.

3.5 TESTING METHODOLOGIES

Integral to information systems implementation is the proper selection of testing methodologies, the development of testing plans fully traceable to requirements and the acquisition of essential resources to successfully complete testing. Once completed, testing provides confidence to stakeholders that a system or system component operates as intended and delivers the benefits realization as required at the start of project.

An IS auditor should understand the application of various forms of testing.

An IS auditor should also understand how QA monitoring and evaluation

contribute to the quality of an organization's internal processes (e.g., project management, software development process or IT service) and the quality of the final products produced by these processes (e.g., the system implemented or software developed).

Testing is an essential part of the systems development process that verifies and validates that a program, subsystem or application performs the functions for which it has been designed. Testing also determines whether the units being tested operate without any malfunction or adverse effect on other components of the system.

The variety of systems development methodologies and organizational requirements provide for a large range of testing schemes or levels. Each set of tests is performed with a different set of data and under the responsibility of different people or functions. An IS auditor plays a preventive or detective role in the testing process.

3.5.1 TESTING CLASSIFICATIONS

The following tests relate, to varying degrees, to the approaches that can be performed based on the size and complexity of the modified system:

• **Unit testing**—The testing of an individual program or module. Unit testing uses a set of test cases that focus on the control structure of the procedural design. These tests ensure that the internal operation of the program performs according to specification.

• **Interface or integration testing**—A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit-tested modules and build an integrated structure dictated by design. The term "integration testing" is also used to refer to tests that verify and validate the functioning of the application under test with other systems, in which a set of data is transferred from one system to another.

• **System testing**—A series of tests designed to ensure that modified programs, objects, database schema, etc., which collectively constitute a new or modified system, function properly. These test procedures are often performed in a nonproduction test/development environment by software developers designated as a test team. The following specific analyses may be carried out during system testing:

– Recovery testing—Checking the system's ability to recover after a software or hardware failure

– Security testing—Making sure the modified/new system includes

provisions for appropriate access controls and does not introduce any security holes that might compromise other systems

– Load testing—Testing an application with large quantities of data to evaluate its performance during peak hours

– Volume testing—Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of

records (data) the application can process

– Stress testing—Studying the impact on the application by testing with an incremental number of concurrent users/services on the application to determine the maximum number of concurrent users/services the

application can process

– Performance testing—Comparing the system's performance to other equivalent systems using well-defined benchmarks

• **Final acceptance testing**—Performed after the system staff is satisfied with the system tests. Acceptance testing occurs during the implementation phase. During this testing phase, the defined methods of testing to apply should be incorporated into the organization's QA methodology. QA activities should proactively encourage that adequate levels of testing be performed on all software development projects. Final acceptance testing has two major parts: quality assurance testing (QAT), focusing on technical aspects of the application, and UAT, focusing on functional aspects of the application. QAT and UAT have different objectives and, therefore, should not be combined.

QAT focuses on the documented specifications and the technology

employed. It verifies that the application works as documented by testing the logical design and the technology itself. It also ensures that the application meets the documented technical specifications and deliverables. QAT is performed

primarily by the IT department. The participation of the end user is minimal and on request. QAT does not focus on functionality testing.

UAT supports the process of ensuring that the system is production-ready and satisfies all documented requirements. The methods include:

• Definition of test strategies and procedures

• Design of test cases and scenarios

• Execution of the tests

• Utilization of the results to verify system readiness

Acceptance criteria are defined elements that a deliverable must meet to satisfy the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user's perspective and should use the system in a manner as close to production as

possible. For example, tests may be based around typical, predefined business process scenarios. If a new business process has been developed to accommodate the new or modified system, it should also be tested at this point. A key aspect of testing should also include testers seeking to verify that supporting processes integrate into the application in an acceptable fashion. Successful completion would generally enable a project team to hand over a complete integrated package of application and supporting procedures.

Ideally, UAT should be performed in a secure testing or staging environment.

A secure testing environment, in which both source code and executable code are protected, helps to ensure that unauthorized or last-minute changes are not made to the system without going through the standard system maintenance process. The nature and extent of the tests will be dependent on the magnitude and complexity of the system change.

Even though acquired systems are tested by the vendor prior to distribution, these systems and any subsequent changes should be tested thoroughly by the end user and the system maintenance staff. These supplemental tests will help ensure that programs function as designed by the vendor and the changes do not interact adversely with existing systems. In the case of acquired software, after

attending to the changes during testing by the vendor, the accepted version should be controlled and used for implementation. In the absence of controls, the risk of introducing malicious patches/Trojan horse programs is very high.

Some organizations rely on integrated test facilities (ITFs). Test data usually are processed in production-like systems. This confirms the behavior of the new application or modules in real-life conditions. These conditions include peak volume and other resource-related constraints. In this environment, IS

will perform tests with a set of fictitious data whereas client representatives use extracts of production data to cover the most possible scenarios as well as some fictitious data for scenarios that would not be tested by the production data. In some organizations that use a subset of production data in a test environment, such production data may be altered to scramble the data so that the confidential nature of the data is obscured from the tester. This is often the case when the acceptance testing is done by team members who, under

usual circumstances, would not have access to such production data.

Once acceptance testing is complete, a certification and accreditation process is performed after the system is implemented and in operation for some time to produce the evidence needed for these processes. This process includes evaluating program documentation and testing effectiveness and results in a final decision for deploying the business application system. For information security issues, the evaluation process includes reviewing security plans, the risk assessments performed and test plans, and the evaluation process results in an assessment of the effectiveness of the security controls and processes to be deployed. Generally involving security staff and the business owner of the application, this process provides some degree of accountability to the business owner regarding the state of the system that he/she will accept for deployment.

When the tests are completed, an IS auditor should issue an opinion to management as to whether the system meets the business requirements, has implemented appropriate controls, and is ready to be migrated to production.

This report should specify the deficiencies in the system that need to be corrected and should identify and explain the risk that the organization is taking by implementing the new system.

Other Types of Testing

Other types of testing include the following:

• **Alpha and beta testing**—The two phases of testing software undergoes before being considered finished. The first stage, called alpha testing, is often performed only by users within the organization developing the software (i.e., systems testing). The second stage, called beta testing, a form of UAT, generally involves a limited number of external users. This involves real-world exposure, sending the beta version of the product to independent test sites or offering it free to interested users.

• **Pilot testing**—A preliminary test that focuses on specific and predetermined aspects of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. POCs are early pilot tests—usually over interim platforms and with only basic functionalities.

• **White box testing**—A test that assesses the effectiveness of software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic paths (i.e., applicable to unit and integration testing). However, testing all possible logic paths in large information systems is not feasible and would be cost-prohibitive; therefore, white box testing is used on a select basis only.

• **Black box testing**—An integrity-based form of testing associated with testing components of an information system's "functional" operating effectiveness without regard to any specific internal program structure. It is applicable to integration (interface) and UAT processes.

• **Function/validation testing**—Similar to system testing but often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements (i.e., Are we building the right product?)

• **Regression testing**—The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be the same as the data used in the original.

• **Parallel testing**—The process of feeding test data into two systems—the modified system and an alternative system (possibly the original system)—

and comparing the results. The purpose of parallel testing is to determine whether the new application performs in the same way as the original system and meets end-user requirements.

• **Sociability testing**—Tests to confirm that the new or modified system can operate in its target environment without adversely impacting existing systems. This should cover the platform that will perform primary application processing and interfaces with other systems and, in a client server or web development, those that perform changes to the desktop environment.

3.5.2 SOFTWARE TESTING

Test plans identify the specific portions of the system to be tested and may include a categorization of types of deficiencies that can be found during the test. Categories of such deficiencies may be system defects, incomplete requirements, designs, specifications, or errors in the test case itself. Test

plans also specify severity levels of problems found, as well as guidelines on identifying the business priority. The tester determines the severity of the problem found during testing. Based on the severity level, the problem may be fixed prior to implementation or may be noted for correction following implementation. The project sponsor, end-user management and the project manager decide early in the test phase on the severity definitions.

Test plans also identify test approaches, such as the following two reciprocal approaches, to software testing:

• **Bottom up**—Testing begins with atomic units, such as programs or modules, and works upward until a complete system testing has taken place. The advantages follow:

– There is no need for stubs or drivers.

– Testing can be started before all programs are complete.

– Errors in critical modules are found early.

• **Top down**—Testing follows the opposite path, either in depth-first or breadth-first search order. The advantages follow:

– Tests of major functions and processing are conducted early.

– Interface errors can be detected sooner.

– Confidence in the system is increased because programmers and users actually see a working system.

Generally, most application testing of large systems follows a bottom-up testing approach that involves ascending levels of integration and testing (e.g., unit or program, subsystem/integration, system):

• **Conduct and report test results**—Describe resources implied in testing, including personnel involved and information resources/facilities used during the test as well as actual versus expected test results. Results reported, along with the test plan, should be retained as part of the system's permanent documentation.

• **Address outstanding issues**—Identify errors and irregularities from the actual tests conducted. When such problems occur, the specific tests in question have to be redesigned in the test plan until acceptable conditions occur when the tests are redone.

3.5.3 DATA INTEGRITY TESTING

Data integrity testing is a set of substantive tests that examines accuracy, completeness, consistency and authorization of data presently held in a system. It employs testing similar to that used for input control. Data integrity tests indicate failures in input or processing controls. Controls for ensuring the integrity of accumulated data in a file can be exercised by regularly checking data in the file. When this checking is done against authorized source documentation, it is common to check only a portion of the file at a time. Because the whole file is regularly checked in cycles, the control technique is often referred to as cyclical checking.

Two common types of data integrity tests are relational and referential integrity tests:

• **Relational integrity tests**—Performed at the data element and record-based levels. Relational integrity is enforced through data validation routines built into the application or by defining the input condition constraints and data

characteristics at the table definition in the database stage. Sometimes it is a combination of both.

• **Referential integrity tests**—Define existence relationships between entities in different tables of a database that needs to be maintained by the DBMS. It is required for maintaining interrelation integrity in the relational data model. Whenever two or more relations are related through referential constraints (primary and foreign key), it is necessary that references be kept consistent in the event of insertions, deletions and updates to these relations. Database software generally provides various built-in automated procedures for checking and ensuring referential integrity. Referential integrity checks involve ensuring that all references to a primary key from another table (i.e., a foreign key) actually exist in their original table. In nonpointer databases (e.g., relational), referential integrity checks involve making sure that all foreign keys exist in their original table.

Data Integrity in Online Transaction Processing Systems In multiuser transaction systems, it is necessary to manage parallel user access to stored data typically controlled by a DBMS and deliver fault tolerance. Of particular importance are four online data integrity requirements known collectively as the ACID principle:

• **Atomicity**—From a user perspective, a transaction is either completed in

its entirety (i.e., all relevant database tables are updated) or not at all. If an error or interruption occurs, all changes made up to that point are backed out.

• **Consistency**—All integrity conditions in the database are maintained with each transaction, taking the database from one consistent state into another consistent state.

• **Isolation**—Each transaction is isolated from other transactions, so each transaction accesses only data that are part of a consistent database state.

• **Durability**—If a transaction has been reported back to a user as complete, the resulting changes to the database survive subsequent hardware or software failures.

3.5.4 APPLICATION SYSTEMS TESTING

Testing the effectiveness of application controls involves analyzing computer application programs, testing computer application program controls, or selecting and monitoring data process transactions. Testing controls by applying appropriate audit procedures is important to ensure their functionality and effectiveness. Methods and techniques for each category are described in **figure 3.20**.

To facilitate the evaluation of application system tests, an IS auditor may also want to use generalized audit software. This is particularly useful when specific application control weaknesses are discovered that affect, for example, updates to master file records and certain error conditions on specific transaction records. Additionally, generalized audit software (GAS) can be used to perform certain application control tests, such as parallel simulation, in comparing expected outcomes to live data.

Figure 3.20—Testing Application Systems			
Analyzing Computer Application Programs			
Technique	**Description**	**Advantages**	**Disadvantages**
Snapshot	• Records flow of designated transactions through logic paths within programs	• Verifies program logic	• Requires extensive knowledge of the IS environment
Mapping	• Identifies specific program logic that has not been tested and analyzes programs during execution to indicate whether program statements have been executed	• Increases efficiency by identifying unused code • Identifies potential exposures	• Cost of software
Tracing and tagging	• Tracing shows the trail of instructions executed during an application. • Tagging involves placing an indicator on selected transactions at input and using tracing to track them.	• Provides an exact picture of sequence of events, and is effective with live and simulated transactions	• Requires extensive amounts of computer time, an intimate knowledge of the application program and additional programming to execute trace routines
Test data/deck	• Simulates transactions through real programs	• May use actual master files or dummies • Source code review unnecessary • Can be used on a surprise basis • Provides objective review and verification of program controls and edits • Initial use can be limited to specific program functions minimizing scope and complexity. • Requires minimal knowledge of the IS environment	• Difficult to ensure that the proper program is checked • Risk of not including all transaction scenarios • Requires good knowledge of application systems • Does not test master file and master file records
Base-case system evaluation	• Uses test data sets developed as part of a comprehensive testing of programs • Verifies correct system operations before acceptance, as well as periodic revalidation	• Comprehensive testing verification and compliance testing	• Extensive effort to maintain data sets • Close cooperation is required among all parties.
Parallel operation	• Processes actual production data through existing and newly developed programs at the same time and compares results and is used to verify changed production prior to replacing existing procedures	• Verifies new system before discontinuing the old one	• Added processing costs
Integrated testing facility	• Creates a fictitious file in the database with test transactions processed simultaneously with live data	• Periodic testing does not require separate test process.	• Need for careful planning • Need to isolate test data from production data
Parallel simulation	• Processes production data using computer programs that simulate application program logic	• Eliminates need to prepare test data	• Programs must be developed.
Transaction selection programs	• Use audit software to screen and select transactions input to the regular production cycle	• Independent of production system • Controlled by the auditor • Requires no modification to production systems	• Cost of development and maintenance

Embedded audit data collection	• Software embedded in host computer applications screens. It selects input transactions and generates transactions during production. Usually, it is developed as part of system development. Types include: – Systems control audit review file (SCARF): Auditor determines reasonableness of tests incorporated into normal processing. It provides information for further review. – Sample audit review file (SARF): Randomly selects transactions to provide representative file for analysis	• Provides sampling and productions statistics	• High cost of development and maintenance • Auditor independence issues
Extended records	• Gathers all data that have been affected by a particular program	• Records are put into one convenient file.	• Adds to data storage costs and overhead, and to system development costs

Automated Application Testing

Test data generators can be used to systematically generate random data that can be used to test programs. The generators work by using the field characteristics, layout and values of the data. In addition to test data generators, there are interactive debugging aids and code logic analyzers available to assist in the testing activities.

3.5.5 IS AUDITOR'S ROLE IN INFORMATION SYSTEMS

TESTING

Testing is crucial in determining that user requirements have been validated, the system is performing as anticipated and internal controls work as intended. Therefore, it is essential that an IS auditor be involved in reviewing this phase and perform the following:

• Review the test plan for completeness; indicate evidence of user participation, such as user development of test scenarios and/or user sign-off of results; and consider rerunning critical tests.

• Reconcile control totals and converted data.

• Review error reports for their precision in recognizing erroneous data and resolution of errors.

• Verify cyclical processing for correctness (month-end, year-end processing,

etc.).

• Verify accuracy of critical reports and output used by management and other stakeholders.

• Interview end users of the system for their understanding of new methods, procedures and operating instructions.

• Review system and end-user documentation to determine its completeness and verify its accuracy during the test phase.

• Review parallel testing results for accuracy.

• Verify that system security is functioning as designed by developing and executing access tests.

• Review unit and system test plans to determine whether tests for internal controls are planned and performed.

• Review the UAT and ensure that the accepted software has been delivered to the implementation team. The vendor should not be able to replace this version.

• Review procedures used for recording and following through on error reports.

3.6 CONFIGURATION AND RELEASE MANAGEMENT

The effective and efficient development and maintenance of complicated IT

systems requires that rigorous configuration, change and release management processes be implemented and adhered to within an organization. These processes provide systematic, consistent and unambiguous control on attributes of IT components comprising the system (hardware, software, firmware, and network connectivity including physical connecting media wire, fiber and radio frequency [RF]). Knowledge of the configuration status of computing environments is critical to system reliability, availability and security along with achieving timely maintenance of these systems. Changes to IT systems must be carefully assessed, planned, tested, approved, documented and communicated to minimize any undesirable consequences to the business processes.

An IS auditor should be aware of the tools available for managing configuration,

change and release management and of the controls in place to ensure SoD between development staff and the production environment.

Because of the difficulties associated with exercising control over both system and programming maintenance activities, more organizations

implement configuration management systems. In many cases, regulatory requirements mandate these levels of control to provide a high degree of reliability and repeatability in all associated system processes. In a configuration management system, maintenance requests must be formally documented and approved by a change control group (e.g., configuration control boards). In addition, careful control is exercised over each stage of the maintenance process via checkpoints, reviews and sign-off procedures.

Configuration management involves procedures throughout the system hardware and software life cycle (from requirements analysis to maintenance) to identify, define and baseline software items in the system and thus provide a basis for problem management, change management and release

management.

The process of checking out prevents or manages simultaneous code edits, with hardware, network and system architects reviewing and approving the changes or updates to both the hardware asset and inventory tracking systems.

Checking in is the process of moving an item to the controlled environment.

When a change is required (and supported by a change control form), the configuration manager will check out the item. Once the change is made, it can be checked using a different version number. The process of checking out also prevents or manages simultaneous code edits. With hardware, network and system architects review and approve the changes or updates to both the hardware asset and the inventory tracking systems.

For configuration management to work, management support is critical. The configuration management process is implemented by developing and following a configuration management plan and operating procedures. This plan should not be limited to just the software developed but should also include all system documentation, test plans and procedures.

Commercial software products are often used to automate some processes.

Such tools should allow control to be maintained for applications software from the outset of system analysis and design to running live. Configuration

management tools will support change management and release management through the:

1. Identification of items affected by a proposed change to assist with impact assessment (functional, operational and security)

2. Recording configuration items affected by authorized changes 3.

Implementation of changes in accordance with authorization records 4. Registering of configuration item changes when authorized changes and releases are implemented

5. Recording of baselines that are related to releases (with known consequences) to which an organization would revert if an implemented change fails

6. Preparing a release to avoid human errors and resource costs

A new version of the system (or builds) should be built only from the baselined items. The baseline becomes the trusted recovery source for these systems and applications.

From an IS audit perspective, effective use of configuration management software provides important evidence of management's commitment to careful control over the maintenance process.

3.7 SYSTEM MIGRATION, INFRASTRUCTURE

DEPLOYMENT AND DATA CONVERSION

New software applications tend to be more comprehensive and integrated than older applications. Furthermore, organizations rely increasingly on data warehouses, models and simulation for decision-making; thus, importing data from old (and legacy) systems into the new application is crucial. Data format, coding, structure and integrity are to be preserved or properly translated. A migration scenario must be set up and a rollback plan needs to be in place. There

are many direct (old to new application) and indirect (using interim repositories) strategies and tools. Data conversion is a one-time task in many development projects. The importance of correct results is critical, and success depends on the use of good practices by the development team as the programmed input checks under development will not be available for the conversion. Source data must be correctly characterized and the destination

database must accommodate all existing data values. Resulting data should be carefully tested. Steps for the conversion that are developed in the test environment must be recorded so they can be repeated on the production system.

An IS auditor should ensure that any tools and techniques selected for the process are adequate and appropriate, data conversion achieves the necessary objectives without data loss or corruption, and any loss of data is both minimal and formally accepted by user management.

3.7.1 DATA MIGRATION

A data conversion (also known as data porting) is required if the source and target systems use different field formats or sizes, file/database structures, or coding schemes. For example, a number may be stored as text, floating point or binary-coded-decimal.

Conversions are often necessary when the source and target systems are on different hardware and/or OS platforms, and different file or database structures (e.g., relational database, flat files, virtual storage access method) are used.

The objective of data conversion is to convert existing data into the new required format, coding and structure while preserving the meaning and integrity of the data. The data conversion process must provide some means, such as audit trails and logs, to allow for the verification of the accuracy and completeness of the converted data. This verification of accuracy and completeness may be performed through a combination of manual processes, system utilities, vendor tools and one-time-use special applications.

A large-scale data conversion can potentially become a project within a project as considerable analysis, design and planning will be required.

Among the steps necessary for a successful data conversion are:

• Determining what data should be converted using programs and what, if any, should be converted manually

• Performing any necessary data cleansing ahead of conversion

• Identifying the methods to be used to verify the conversion, such as

automated file comparisons, comparing record counts and control totals, accounting balances, and individual data items on a sample basis

• Establishing the parameters for a successful conversion (e.g., Is 100 percent consistency between the old and new systems necessary, or will some differences within defined ranges be acceptable?)

• Scheduling the sequence of conversion tasks

• Designing audit trail reports to document the conversion, including data mappings and transformations

• Designing exception reports to record any items that cannot be converted automatically

• Establishing responsibility for verifying and signing off on individual conversion steps and accepting the overall conversion

• Developing and testing conversion programs, including functionality and performance

• Performing one or more conversion dress rehearsals to familiarize persons with the sequence of events and their roles, and testing the conversion process end to end with real data

• Controlling the outsourcing of the conversion process with a proper agreement covering nondisclosure, data privacy, data destruction and other warranties

• Running the actual conversion with all necessary personnel onsite or able to be contacted

A successful data migration delivers the new system on time, on budget and with the required quality. The data migration project should be carefully planned and

use appropriate methodologies and tools to minimize the risk of:

• Disruption of routine operations

• Violation of the security and confidentiality of data

• Conflicts and contention between legacy and migrated operations

• Data inconsistencies and loss of data integrity during the migration process The data model and the new application model should be stored in an enterprise repository. Using a repository allows a simulation of the migration scenario and traceability during the project. An enterprise repository enables an overview of the reengineering and data migration process (e.g., which modules and entities are in which stage, such as in service or already

migrated). These models will be modified in the course of the processes described in the following sections.

Refining the Migration Scenario

In order to determine the scope of the implementation project, module analysis should be undertaken to identify the affected functional modules and data entities. The plan of the implementation project should be refined based on this information and an analysis of business requirements.

The next step is to develop a migration plan. This is a detailed listing of tasks for the production deployment of a new system. Within this plan decision points are defined to make “go” or “nogo” decisions. The following processes require decision points:

• **Support migration process**—A support process to administer the enterprise repository must be implemented. Because this repository should be used on completion of the project to manage the software components of the new architecture, this process should be capable of supporting future development processes. The enterprise repository administration and report generation support the migration by supporting the reverse engineering of changes in the legacy architecture and facilitating the creation of impact analysis reports.

• **Migration infrastructure**—The project develops specifications for the infrastructure of the migration project. This approach ensures consistency and

increases confidence in the functionality of the fallback scenario. The migration project team completes a high-level analysis of the legacy and new data models to establish links between them that will be refined later.

The migration infrastructure is the basis for specifying the following components:

– Data redirector (temporary adapters)—Good practices suggest the staged deployment of applications to minimize the end-user impact of their implementation and limit the risk by having a fallback scenario with minimum impact. For this reason, an infrastructure component is needed to handle distributed data on different platforms within distributed applications. The design of a data redirector on the new architecture corresponds to service-oriented architectures and should cover features such as access to the not-yet-migrated legacy data during run time, data

consistency due to the usage of standards such as X/Open XA interface, and a homogeneous new architecture.

– Data conversion components—The need to create an enterprise data model to eliminate data redundancies and inconsistencies often is identified. For this reason, infrastructure components to transform the legacy data model to the new data model must be provided. These

components can be described as follows:

• Unload components to copy the data (either as is or suitably modified to align with the data format of target system) in legacy databases that have been identified for migration

• Transfer components to execute the data transfer from the legacy system to the new system

• Load components to execute the load of the data into the new database
Software packages that support data migration, such as ERP and document management software, should be acquired as soon as the software evaluation is done. The data conversion plan should be based on the available databases and migration tools provided by the selected vendor(s).

The decision on which method to use for data conversion has to be made as part

of the implementation project and should be based transaction volume and change degree of the data model.

Fallback (Rollback) Scenario

Not all new system deployments go as planned. To mitigate the risk of downtime for mission-critical systems, good practices dictate that the tools and applications required to reverse the migration are available prior to attempting the production cutover. Some or all of these tools and applications may need to be developed as part of the project.

Components have to be delivered that can back out all changes and restore data to the original applications in the case of nonfunctioning new applications. Two types of components should be considered as part of a fallback contingency plan.

The first consists of:

• Unload components to execute the unloading of the data from the new data structures

• Transfer components for the data conversion

• Load components to execute the loading of the data into the legacy data structures

The second consists of:

• A log component to log the data modifications within the new data model during runtime within the service layer

• Transfer components for the data conversion

• Load components to execute the load of the data into the legacy data structures

Another important consideration is the new system’s data structure. This can be determined by reading the software user guides, analyzing the entity relationship diagrams, understanding the relationships between data elements and reviewing definitions of key terms (such as “entity” and “record”) in the new system.

Next, it is important to review the decisions on how business processes should

be conducted in the new system. Changes are identified, and the output of this exercise is a table of new data terminology against current definitions of data elements. In this step, the project team identifies how current data are defined in the new system. Following this step, a data cleanup is completed to eliminate inconsistencies in the current database, if possible, and duplications of data sets are discovered and resolved. The rules of conversion are defined and documented, with the objective of ensuring the business processes executed in the new system yield results that maintain data integrity and relationships.

Data conversion rules are programmed by the software development team.

Data conversion scripts are created to convert the data from the old database to the new database. These are tested on a discrete selection of data that is carefully selected to include all cases. This process is referred to as

“program” or “unit testing.” Following the sign-off of data conversion scripts by programmers, the scripts are run on a test copy of the production database.

The values of data are verified by executing assessments including business process tests. Users and developers complete cycles of testing until conversion scripts are fine-tuned. After testing has been completed, the next step is to promote the converted database to production.

The key points to be taken into consideration in a data conversion project are to ensure:

• Completeness of data conversion

• Integrity of data

• Storage and security of data under conversion

• Consistency of data

• Continuity of data access

The last copy of the data before conversion from the old platform and the first copy of the data after conversion to the new platform should be maintained separately in the archive for any future reference.

3.7.2 CHANGEOVER (GO-LIVE OR CUTOVER)

TECHNIQUES

Changeover refers to an approach to shift users from using the application from the existing (old) system to the replacing (new) system. This is appropriate only after testing the new system with respect to its program and relevant data. This is sometimes called the “go-live” technique because it enables the start of the new system. This approach is also called the “cutover”

technique because it helps in cutting out from the older system and moving over to the newer system.

This technique can be achieved in three different ways.

Parallel Changeover

This technique includes running the old system, then running both the old and new systems in parallel, and, finally, fully changing over to the new system after gaining confidence in the working of the new system. With this approach, the users will have to use both systems during the period of overlap. This will minimize the risk of using the newer system and, at the same time, help in identifying problems, issues or any concerns that the user

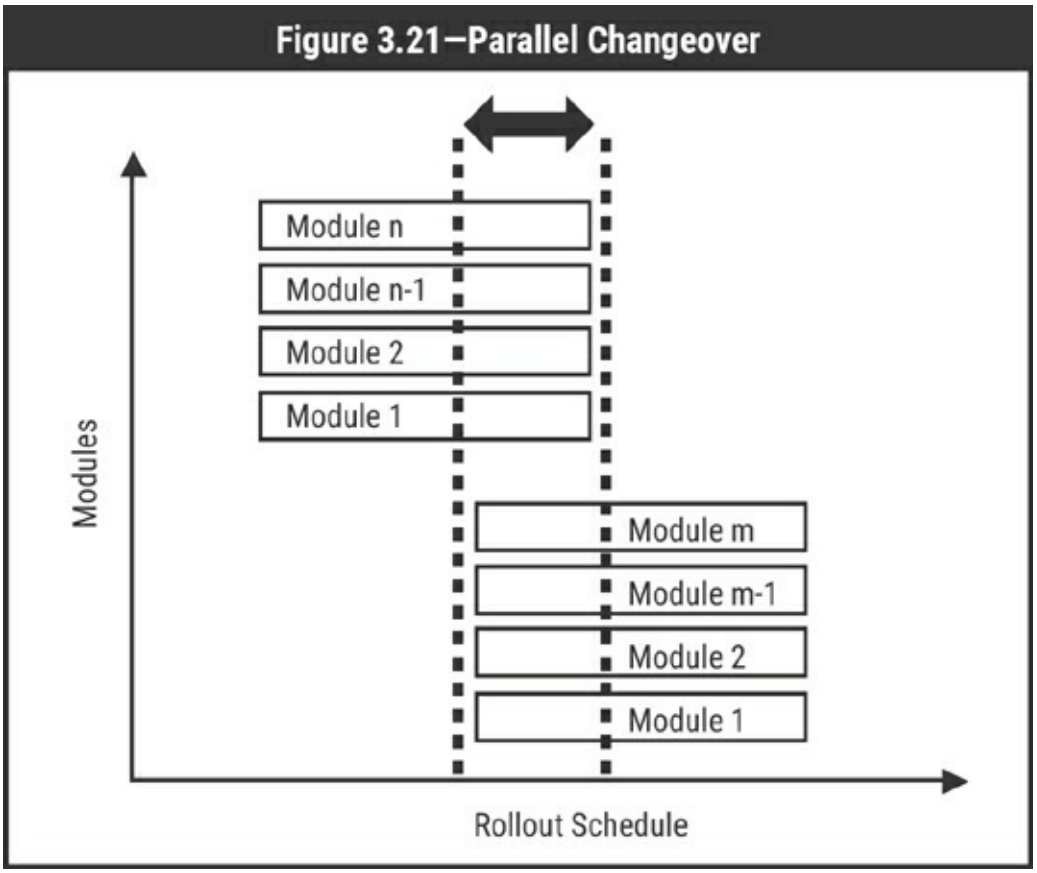


Figure 3.21—Parallel Changeover

comes across in the newer system in the beginning. After a period of overlap, the user gains confidence and assurance in relying on the newer system. At this point, the use of the older system is discontinued, and the new system becomes totally operational. Note in **figure 3.21** that the number (m, n, respectively) of modules in the new and old systems may be different.

Phased Changeover

In this approach the older system is broken into deliverable modules.

Initially, the first module of the older system is phased out using the first module of the newer system. Then, the second module of the older system is phased out, using the second module of the newer system, and so forth until reaching the last module. Thus, the changeover from the older system to the newer system takes place in a preplanned, phased manner. See **figure 3.22.**

Some of the risk that may exist in the phased changeover includes:

• Resource challenges (both on the IT side—to be able to maintain two

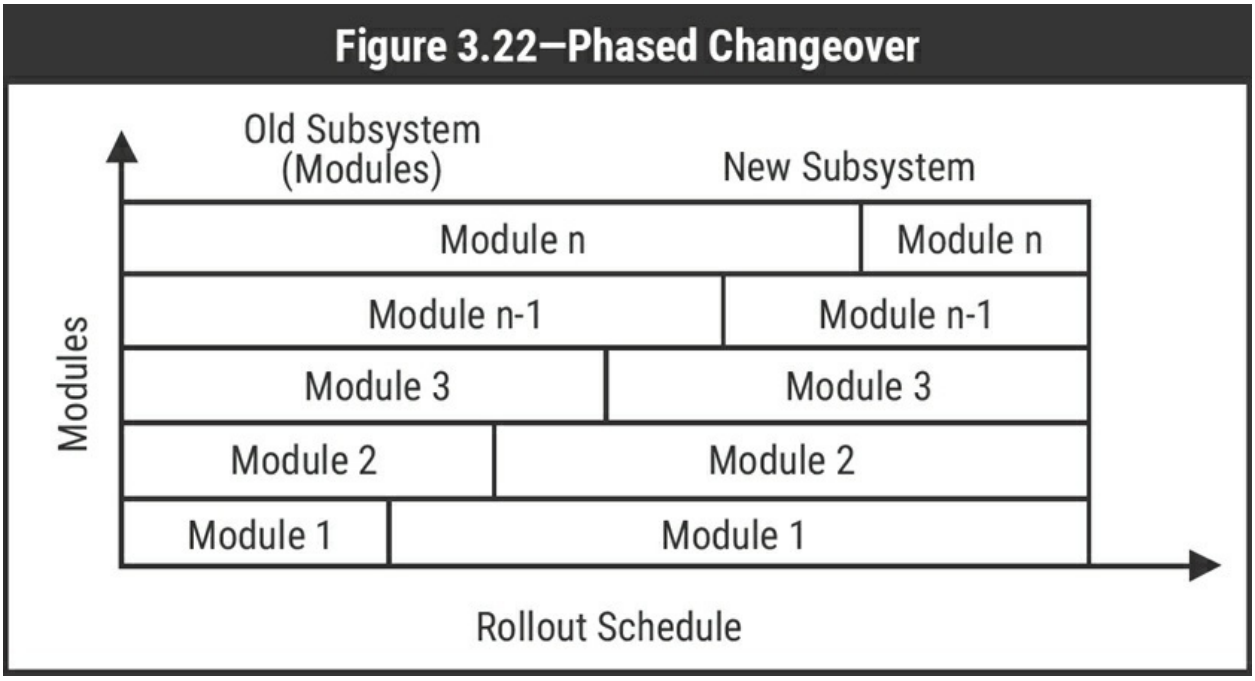


Figure 3.22—Phased Changeover

unique environments such as hardware, OSs, databases and code; and on the operations side—to be able to maintain user guides, procedures and policies, definitions of system terms, etc.)

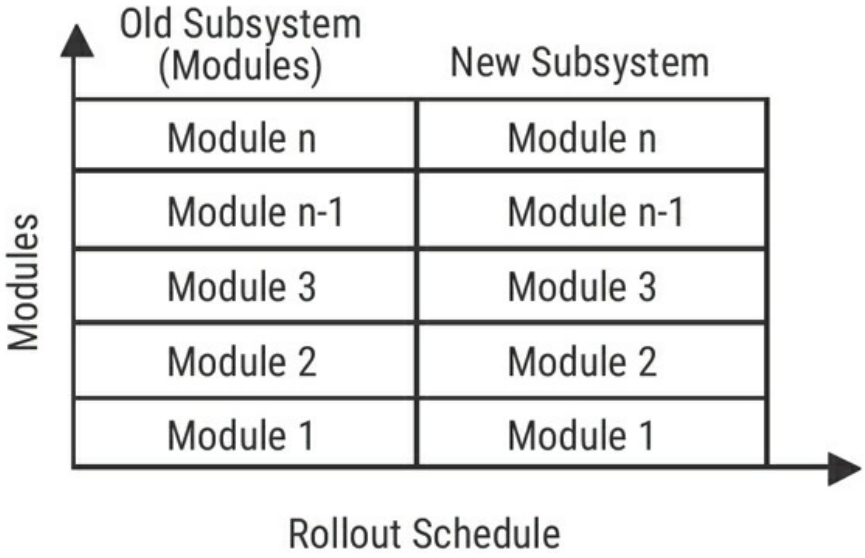
• Extension of the project life cycle to cover two systems

• Change management for requirements and customizations to maintain ongoing support of the older system

Abrupt Changeover

In this approach the newer system is changed over from the older system on a cutoff date and time, and the older system is discontinued once changeover to the new system takes place. See **figure 3.23**.

Figure 3.23—Abrupt Changeover



Changeover to the newer system involves four major steps or activities: 1. Conversion of files and programs; test running on test bed

2. Installation of new hardware, OS, application system and the migrated data

3. Training employees or users in groups

4. Scheduling operations and test running for go-live or changeover Some of the risk items related to changeover include:

• Asset safeguarding

• Data integrity

• System effectiveness

• System efficiency

• Change management challenges (depending on the configuration items considered)

• Duplicate or missing records (possible existence of duplicate or erroneous records if data cleansing is not done correctly)

3.7.3 SYSTEM IMPLEMENTATION

Implementation is initiated only after a successful testing phase. The system should be installed according to the organization’s change control

procedures.

An IS auditor should verify that appropriate sign-offs have been obtained prior to implementation and perform the following:

• Review the programmed procedures used for scheduling and running the system along with system parameters used in executing the production schedule.

• Review all system documentation to ensure its completeness and confirm that all recent updates from the testing phase have been incorporated.

• Verify all data conversions to ensure that they are correct and complete before implementing the system in production.

Implementation Planning

Once developed and ready for operation, the new system delivered by the project will need an efficient support structure. It is not enough to set up roles for a support structure and name people to fulfill these roles. Support personnel will need to acquire new skills. Workload has to be distributed, in order for the right people to support the right issues; thus, new processes have to be developed while respecting the specificities of IT department requirements. Additionally, an infrastructure dedicated for support staff has to be made available. For these and other reasons, setting up a support structure normally is a project in itself and requires planning, a methodology and good practices adaptation from past experiences.

The objective of such a project is to develop and establish the to-be support structure for the new technical infrastructure. The main goals are to accomplish the following:

• Provide appropriate support structures for first-, second- and third-line support teams.

• Provide a single point of contact.

• Provide roles and skills definitions with applicable training plans.

Often the project sponsor’s organization operates and supports a legacy solution and will implement a new system environment based on new system architecture. The existing support procedures and the organizational units will have to maintain the future system to provide the appropriate level of support

for the new platform as well as for the old one.

To achieve significant success in updating staff on changes to the business process and introducing new software, it is necessary to address some important questions such as:

• How can the existing support staff be involved in the setup of the new project without neglecting the currently running system?

• What is the gap of knowledge/skills that must be addressed in the training plan?

• How large is the difference from the current legacy environment operation to the operation of the new platform?

Generally, a transition project should conform to the following guidelines:

• There should be a smooth transition from the existing platform to the new platform, without any negative effect on users of the system.

• There should be maximum employment of the existing support staff to operate the new system environment and keep the effort of new hires at a minimum level.

A primary challenge is to manage the phases from build, to integrate, to migrate, and for the phasing-out of the existing system and the phasing-in of the new one. The migration cannot be accomplished via a single event.

Instead, a step-by-step transition of the affected services must take place.

Further, the implemented processes for a legacy environment might be different from what may be implemented with the new platform and any changes must be communicated to users and system support staff.

Implementation Plan/Knowledge Transfer Plan

In accordance with good practices, the transfer should follow the shadowing and relay-baton method. Shadowing gives staff the opportunity to become accustomed to the system by observation. The relay-baton approach is the best suitable concept to transfer knowledge and also to transfer responsibility in a transparent way. The metaphor of the relay-baton expresses exactly what must be achieved—that is, knowledge is transferred in small portions.

Training Plan

After the roles and responsibilities are defined, they will be documented in the form of a chart to allow for a clear and easy-to-read overview.

For example, a staff training plan should show all of the required training in terms of:

• Content

• Scheduling information

• Duration

• Delivery mechanism (classroom and/or web-based)

• Train-the-trainer concept

The plan should consider the role definitions and skill profiles for the new to-be structure, and the results of the gap analysis. The plan considers that the staff who need to be trained must still run the current system, so a detailed coordination with the daily business tasks is maintained.

The following list gives an example of work tasks defined to fulfill the overall project goal:

• Collate existing support structure documentation.

• Review the existing IT organization model.

• Define the new support organization structure.

• Define the new support processes.

• Map the new process to the organization model.

• Execute the new organization model.

• Establish support functions.

• Develop communications material for support staff.

• Conduct briefing and training sessions.

• Review mobilization progress.

• Transfer to the new organization structure.

• Review the preceding items.

3.7.4 SYSTEM CHANGE PROCEDURES AND THE PROGRAM MIGRATION PROCESS

Following implementation and stabilization, a system enters into the ongoing development or maintenance stage. This phase continues until the system is retired. The phase involves those activities required to either correct errors in the system or enhance the capabilities of the system.

In this regard, an IS auditor should consider the following:

• The existence and use of a methodology for authorizing, prioritizing and tracking system change requests from the user

• Whether emergency change procedures are addressed in the operations manuals

• Whether change control is a formal procedure for the user and the development groups

• Whether the change control log ensures all changes shown were resolved

• The user’s satisfaction with the turnaround—timeliness and cost—of change requests

• The adequacy of the security access restrictions over production source and executable modules

• The adequacy of the organization’s procedures for dealing with emergency program changes

• The adequacy of the security access restrictions over the use of the emergency logon IDs

For a selection of changes on the change control log:

• Determine whether changes to requirements resulted in appropriate change-development documents, such as program and operations documents.

• Determine whether changes were made as documented

• Determine whether current documentation reflects the changed

environment.

• Evaluate the adequacy of the procedures in place for testing system changes.

• Review evidence (test plans and test results) to ensure that procedures are carried out as prescribed by organizational standards.

• Review the procedures established for ensuring executable and source code integrity.

• Review production executable modules and verify there is one and only one corresponding version of the program source code.

• Check the technical controls of the change management tool.

Additionally, an IS auditor should review the overall change management

process for possible improvements in acknowledgment, response time, response effectiveness and user satisfaction with the process.

Critical Success Factors

Critical success factors of planning the implementation include the following:

• To avoid delays, the appropriate skilled staff must attend workshops and participate for the entire project duration.

• The documentation needed for carrying out the work needs to be ready at project initiation.

• Decision-makers must be involved at all steps to ensure all necessary decisions can be made.

End-user Training

The goal of a training plan is to ensure that the end user can become self-sufficient in the operation of the system. One of the most important keys in end-user training is to ensure that training is considered and a training project plan is created early in the development process. A strategy can be developed that would take into consideration the timing, extent and delivery mechanisms.

The training should be piloted using a cross-section of users to determine how best to customize the training to the different user groups. Following the pilot, the training approach can be adjusted as necessary, based on the feedback received from the pilot group.

Separate classes should be developed for individuals who will assist in the training process. These train-the-trainer classes also provide useful feedback for improving the content of the training program.

The timing of the delivery of training is very important. If training is delivered too early, users will forget much of the training by the time the system actually goes into production. If training is delivered too late, there will not be enough time to obtain feedback from the pilot group and implement the necessary changes into the main training program. Training classes should be customized to address skill level and needs of users based on their role within the organization.

To develop the training strategy, an organization must name a training administrator. The training administrator will identify users who need to be

trained with respect to their specific job functions. Consideration should be given to the following format and delivery mechanisms:

• Case studies

• Role-based training

• Lecture and breakout sessions

• Modules at different experience levels

• Practical sessions on how to use the system

• Remedial computer training (if needed)

• Online sessions on the web or on a CD-ROM

It is important to have a library of cases or tests, including user errors and the system response to those errors. The training administrator should record student information in a database or spreadsheet, including student feedback for improving the training course.

3.7.5 SYSTEM SOFTWARE IMPLEMENTATION

System software implementation involves identifying features, configuration options and controls for standard configurations to apply across the organization. Additionally, implementation involves testing the software in a nonproduction environment and obtaining some form of certification and accreditation to place the approved OS software into production.

3.7.6 CERTIFICATION/ACCREDITATION

Certification is a process by which an assessor organization performs a comprehensive assessment against a standard of management and operational and technical controls in an information system. The assessor examines the level of compliance in meeting certain requirements such as standards, policies, processes, procedures, work instructions and guidelines—

requirements made in support of accreditation. The goal is to determine the extent to which controls are implemented correctly, operating as intended and

producing the desired outcome with respect to meeting the system's security requirements. The results of a certification are used to reassess the risk and update the system security plan, thus providing the factual basis for an

authorizing official to render an accreditation decision.

Accreditation is the official management decision (given by a senior official) to authorize operation of an information system and to explicitly accept the risk to the organization's operations, assets or individuals based on the implementation of an agreed-upon set of requirements and security controls.

Security accreditation provides a form of QC and challenges managers and technical staff at all levels to implement the most effective security controls possible in an information system, given mission requirements, and technical, operational and cost/schedule constraints.

By accrediting an information system, a senior official accepts responsibility for the security of the system and is fully accountable for any adverse impact to the organization if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize accreditation.

3.8 POST-IMPLEMENTATION REVIEW

Projects should be formally closed to provide accurate information on project results, improve future projects and allow an orderly release of project resources. The closure process should determine whether project objectives were met or excused and should identify lessons learned to avoid mistakes and encourage repetition of good practices. In contrast to project closure, a post-implementation review typically is carried out in several weeks or months after project completion, when the major benefits and shortcomings of the solution implemented will be realized. The review is part of a benefits realization process and includes an estimate of the project's overall success and impact on the business.

A post-implementation review is also used to determine whether appropriate controls were built into the system. It should consider both the technical details and the process that was followed in the course of the project, including the following:

• Adequacy of the system:

– Does the system meet user requirements and business objectives?

– Have controls been adequately defined and implemented?

• Projected cost versus benefits or ROI measurements

• Recommendations that address any system inadequacies and deficiencies

• Plan for implementing any recommendations

• Assessment of the development project process:

– Were the chosen methodologies, standards and techniques followed?

– Were appropriate project management techniques used?

– Is the risk of operating the system within acceptable risk levels?

Not all lessons associated with a given project may be immediately evident upon completion. It is good practice for the project development team and a selection of end users to perform a second, joint review after the project has been completed and the system has been in production for a sufficient time period to assess its effectiveness and value to the organization.

Closing a project is a formal process that focuses on capturing lessons learned for future use. **Figure 3.24** summarizes five steps that should be included in the closing of a project.

It is important to note that, for a post-implementation review to be effective, the information to be reviewed should be identified during the project feasibility and design phase, and collected during each stage of the project.

For instance, the project manager might establish certain checkpoints to measure effectiveness of software development processes and accuracy of software estimates during the project execution. Business measurements should also be established up front and collected before the project begins and after the project is implemented (for examples of CSF measurements, see

figure 3.25).

It is also important to allow a sufficient number of business cycles to be executed in the new system to realize the new system's actual ROI.

A post-implementation project review should be performed jointly by the project development team and appropriate end users. Typically, the focus of this type of internal review is to assess and critique the project process, whereas a post-implementation review has the objective of assessing and measuring the value the project has on the business. Alternatively, an

independent group not associated with the project implementation (internal or external audit) can perform a post-implementation review.

Figure 3.24—Project Closeout Steps

Step	**Action**
1	Assign responsibility for any outstanding issues to specific individuals and identify the related budget for addressing these issues (if applicable).
2	Assign custody of contracts, and either archive documentation or pass it on to those who need it.
3	Conduct a post-implementation review with the project team, development team, users and other stakeholders to identify lessons learned that can be applied to future projects. Include the following information: • Content-related criteria, such as: – Fulfillment of deliverable targets and any additional objectives −

Attainment of project-related incentives

– Adherence to the schedule and costs

• Process-related criteria, such as:

– Team dynamics and internal communication

– Relationships between the project team and external stakeholders 4

Document any risk that was identified in the course of the project, including risk that may be associated with proper use of the

deliverables, and update the risk register.

5

Complete a second post-implementation review after the project

deliverables have been completed for long enough to realize the true business benefits and costs, and use the results of this review to measure the project's overall success and impact on the business.

Figure 3.25—Measurements of Critical Success Factors

Productivity

Dollars spent per user

Number of transactions per month

Number of transactions per user

Quality

Number of discrepancies

Number of disputes

Number of occurrences of fraud/misuse detection

Economic value

Total processing time reduction

Monetary value of administration costs

Customer service

Turnaround time for customer question handling Frequency of useful communication to users

3.8.1 IS AUDITOR'S ROLE IN POST-IMPLEMENTATION REVIEW

An IS auditor performing a post-implementation review should be

independent of the system development process. Therefore, an IS auditor involved in consulting with the project team on the development of the system should not perform this review. Unlike internal project team reviews, post-implementation reviews performed by an IS auditor tend to concentrate on the control aspects of the system development and implementation processes.

It is important that all audit involvement in the development project be thoroughly documented in the audit work papers to support an IS auditor's findings and recommendations. This audit report and documentation should be reused during maintenance and changes to validate, verify and test the impact of any changes made to the system. The system should periodically undergo a review to ensure the system is continuing to meet business objectives in a cost-effective manner and control integrity still exists.

Note: The CISA candidate should be familiar with issues related to dual controls as they apply to authorization within the post-implementation review and with those related to reviewing results of live processing.

An IS auditor should perform the following functions:

• Determine if the system's objectives and requirements were achieved.

During the post-implementation review, careful attention should be paid to the

end users' utilization, trouble tickets, work orders and overall satisfaction with the system. This will indicate whether the system's objectives and requirements were achieved.

• Determine if the cost benefits identified in the feasibility study are being measured, analyzed and accurately reported to management.

• Review program change requests performed to assess the type of changes required of the system. The type of changes requested may indicate problems in the design, programming or interpretation of user

requirements.

• Review controls built into the system to ensure that they are operating according to design. If an EAM was included in the system, this module should be used to test key operations.

• Review operators' error logs to determine if there are any resource or operating problems inherent within the system. The logs may indicate inappropriate planning or testing of the system prior to implementation.

• Review input and output control balances and reports to verify that the system is processing data accurately.

CASE STUDY

Wonderwheels is a major national retailer specializing in outdoor sports, hunting, fishing and camping, including a wide variety of all-terrain vehicles (ATVs), which inspired its name. The company has operations currently based in the United States and has a long-term business plan to expand its retail centers to selected parts of the European Union (EU).

As part of ongoing current operations, management has asked an internal IS

auditor to review the company's readiness for complying with requirements for protecting cardholder information. This is meant to be a high-level overview of where the firm stands and not a point-by-point review of its compliance with the specific standard (which would be undertaken as a separate engagement later in the year).

During the initial assessment, the IS auditor learned the following information:

• **Point-of-sale (POS) register encryption**—The retailer uses wireless POS

registers that connect to application servers located at each store. These registers use wired equivalent protection (WEP) encryption.

• **POS local application server locations**—The POS application server, usually located in the middle of each store's customer service area, forwards all sales data over a frame relay network to database servers located at the retailer's corporate headquarters, with strong encryption applied to the data, which are then sent over a virtual private network (VPN) to the credit card processor for approval of the sale.

• **Corporate database locations**—Corporate databases are located on a protected screened subset of the corporate local area network.

• **Sales data distribution**—Weekly aggregated sales data, by product line, are copied as-is from the corporate databases to magnetic media and mailed to a third party for analysis of buying patterns.

• **Current ERP system compliance**—The current state of the company's ERP system is such that it may be out of compliance with newer laws and

regulations. During the initial assessment, the IS auditor determined that the ERP system does not adhere to the EU's General Data Protection Regulation (GDPR).

Additionally, Wonderwheels' database software has not been patched in over two years, due to a few factors:

• The vendor's support for the database package was dropped due to it being acquired by a competitor and refocusing the remaining business to other software services.

• Wonderwheels' management has implemented plans to upgrade to a new database package. The upgrade is underway; however, it is taking longer than anticipated.

Regarding the database upgrade, sizeable customizations were anticipated and are being carried out with a phased approach of partial deliverables.

These deliverables are released to users for pilot usage on real data and actual projects. Concurrently, design and programming of the next phase are ongoing. In spite of positive initial test results, the internal audit group has voiced that it has not been included in key compliance decisions regarding the configuration and testing of the new system. In addition, operational transactions are often queued, or “hang” during execution, and more and more frequently, data are corrupted in the database. Additional problems have shown up—errors already corrected have started occurring again and functional modifications already tested tend to present other errors. The project, already late, is now in a critical situation.

1.

Which of the following would present the **MOST** significant risk to the retailer?

A. Database patches are severely out of date.

B. Wireless POS registers use WEP encryption.

C. Credit cardholder information is sent over the Internet.

D. Aggregate sales data are mailed to a third party.

2.

Based on the case study, which of the following controls would be the **MOST** important to implement?

A. POS registers should use two-factor authentication, with enforced complex passwords.

B. Wireless access points should use MAC address filtering.

C. The current ERP system should be patched for compliance with

GDPR.

D. Aggregate sales data should be anonymized and encrypted prior to distribution.

3.

In the preliminary report to management, regarding the state of the database upgrade, which of the following is **MOST** important for the IS

auditor to include?

A. Internal audit should be included among the steering committee approvals.

B. There is a possibility that the new database may not be compatible with the existing ERP solution.

C. An ERP upgrade and/or patch is required in order to ensure updated database compatibility.

D. Internal audit should be able to review the upgraded database to ensure compliance with Payment Card Industry Data Security

Standard (PCI-DSS).

4.

In order to contribute more directly to help address the problems around the database upgrade, the IS auditor should:

A. Review the validity of the functional project specifications as the basis for an improved software baselining definition.

B. Propose to be included in the project team as a consultant for QC of deliverables.

C. Research the problems further to identify root causes and define appropriate countermeasures.

D. Contact the project leader and discuss the project plans and

recommend redefining the delivery schedule using the PERT

methodology.

ANSWERS TO CASE STUDY QUESTIONS

1.

A.

Unpatched database servers are located on a screened subnet; this would mitigate the risk to the organization.

B.

Use of WEP encryption would present the most significant

risk because WEP uses a fixed secret key that is easy to break.

Transmission of credit cardholder information by wireless

registers would be susceptible to interception and would

present a very serious risk.

C.

Sending credit cardholder data over the Internet would be less of a risk because strong encryption is being used.

D.

Because the sales data being sent to the third party are aggregate data, no cardholder information should be included.

2.

A.

According to the case study, it is unclear whether or not the POS

registers already use two-factor authentication. It is known that aggregate sales data are copied onto other media as-is, without

any controls, for external distribution.

B.

According to the case study, it is unclear whether or not the

wireless access points use MAC address filtering. It is known that aggregate sales data are copied onto other media as-is, without

any controls, for external distribution.

C.

Compliance with the GDPR, while important, is not the most

important due to the current operations being only in the US, and the potential for expansion into the EU is a long-term vision for the company.

D.

It is unclear whether or not sales data are secure and free of personally identifiable information, such as credit card

information and Social Security numbers. This would present

the most significant risk and should be addressed.

3.

A.

If internal audit is part of the steering committee, then it will have a say in the compliance and security-related controls to be included in production releases.

B.

Ensuring database compliance is an operational responsibility

and not an audit responsibility.

C.

Compatibility with existing architecture must be a function of the database implementation project team as a whole, which can

include internal audit and also includes operations. Therefore, it is not the best choice.

D.

While it is important that the upgraded database solution be

compliant with all regulations affecting the company, such a

review should not be limited to one regulation. Therefore, it is not the best choice of those provided.

4.

A.

Functional project specifications should be executed by users and systems analysts, and not by the auditor.

B.

To propose to be project consultant for quality would not bring

about an essential contribution since quality is a formal

characteristic, whereas in the current case, the problem is a

substantial system instability.

C.

The only appropriate action is additional research, even if the apparently technical nature of the problem renders it unlikely that the auditor may find it alone.

D.

To contact the project leader and redesign the schedule of

deliveries would not solve the problem. Furthermore, the

definition of real causes may sensibly alter the project environm

Chapter 4:

Information Systems Operations and

Business Resilience

Overview

Domain 4 Exam Content Outline

Learning Objectives/Task Statements

Suggested Resources for Further Study

Self-assessment Questions

Answers to Self-assessment Questions

Part A: Information Systems Operations

4.0

Introduction

4.1

Common Technology Components

4.2

IT Asset Management

4.3

Job Scheduling and Production Process Automation

4.4

System Interfaces

4.5

End-user Computing

4.6

Data Governance

4.7

Systems Performance Management

4.8

Problem and Incident Management

4.9

Change, Configuration, Release and Patch Management

4.10 IT Service Level Management.

4.11 Database Management

Part B: Business Resilience

4.12 Business Impact Analysis

4.13 System Resiliency

4.14 Data Backup, Storage and Restoration

4.15 Business Continuity Plan

4.16 Disaster Recovery Plans

Case Study

Case Study

Answers to Case Study Questions

OVERVIEW

Information systems operations and business resilience are important to provide assurance to users and management that the expected level of service will be delivered. Service level expectations are derived from the organization's business objectives. Information technology (IT) service delivery includes information systems (IS) operations, IT services and management of IS and the groups responsible for supporting them.

Disruptions are also an often-unavoidable factor of doing business.

Preparation is key to being able to continue business operations while protecting people, assets and reputation. Employing business resiliency tactics helps organizations address these issues and limit the impact.

This domain represents 23 percent of the CISA examination (approximately 34 questions).

DOMAIN 4 EXAM CONTENT OUTLINE

Part A: Information Systems Operations

1. Common Technology Components

2. IT Asset Management

3. Job Scheduling and Production Process Automation

4. System Interfaces

5. End-User Computing

6. Data Governance

7. Systems Performance Management

8. Problem and Incident Management

9. Change, Configuration, Release, and Patch Management

10. IT Service Level Management

11. Database Management

Part B. Business Resilience

1. Business Impact Analysis (BIA)

2. System Resiliency

3. Data Backup, Storage, and Restoration

4. Business Continuity Plan (BCP)

5. Disaster Recovery Plans (DRPs)

LEARNING OBJECTIVES/TASK STATEMENTS

Within this domain, the IS auditor should be able to:

• Evaluate the organization's ability to continue business operations. (T13)

• Evaluate whether IT service management practices align with business requirements. (T20)

• Conduct periodic review of information systems and enterprise

architecture. (T21)

• Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization's objectives. (T22)

• Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization's objectives. (T23)

• Evaluate database management practices. (T24)

• Evaluate data governance policies and practices. (T25)

• Evaluate problem and incident management policies and practices. (T26)

• Evaluate change, configuration, release, and patch management policies and practices. (T27)

• Evaluate end-user computing to determine whether the processes are effectively controlled. (T28)

• Evaluate policies and practices related to asset life cycle management.

(T33)

SUGGESTED RESOURCES FOR FURTHER STUDY

Hobbs, Martyn; IT Asset Management: *A Pocket Survival Guide*, IT

Governance Publishing, USA, 2011.

ISACA, COBIT® 2019, USA, 2018, *www.isaca.org/cobit*

International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 20000-1:2018, *Information technology—Service*

management—Part 1: Service management system requirements, Switzerland, 2018, *www.iso.org/standard/70636.html*

Mullins, Craig S.; *Database Administration: The Complete Guide to DBA Practices and Procedures, 2nd Edition*, Addison-Wesley Professional, USA, 2012

Snedaker, Susan; *Business Continuity & Disaster Recovery for IT*

Professionals 2nd Edition, Syngress Publishing Inc., USA, 2013

Wallace, Michael; Lawrence Webber; *The Disaster Recovery Handbook; A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets, 2nd Edition*, AMACOM, USA, 2010

SELF-ASSESSMENT QUESTIONS

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided. Please note that these questions are not actual or retired exam items. Please see the section

“About This Manual” for more guidance regarding practice questions.

4-1

Which one of the following provides the **BEST** method for determining the level of performance provided by similar information processing facility environments?

A. User satisfaction

B. Goal accomplishment

C. Benchmarking

D. Capacity and growth planning

4-2

For mission critical systems with a low tolerance to interruption and a high cost of recovery, the IS auditor, in principle, recommends the use of which of the following recovery options?

A. Mobile site

B. Warm site

C. Cold site

D. Hot site

4-3

Which of the following is the **MOST** effective method for an IS auditor to use in testing the program change management process?

A. Trace from system-generated information to the change

management documentation

B. Examine change management documentation for evidence of

accuracy

C. Trace from the change management documentation to a system-

generated audit trail

D. Examine change management documentation for evidence of

completeness

4-4

Which of the following would allow an enterprise to extend its intranet across the Internet to its business partners?

A. Virtual private network

B. Client-server

C. Dial-up access

D. Network service provider

4-5

The classification based on criticality of a software application as part of an IS business continuity plan is determined by the:

A. nature of the business and the value of the application to the business.

B. replacement cost of the application.

C. vendor support available for the application.

D. associated threats and vulnerabilities of the application.

4-6

When conducting an audit of client-server database security, the IS

auditor should be **MOST** concerned about the availability of: A. system utilities.

B. application program generators.

C. systems security documentation.

D. access to stored procedures.

4-7

When reviewing a network used for Internet communications, an IS

auditor will **FIRST** examine the:

A. validity of password change occurrences.

B. architecture of the client-server application.

C. network architecture and design.

D. firewall protection and proxy servers.

4-8

An IS auditor should be involved in:

A. observing tests of the disaster recovery plan.

B. developing the disaster recovery plan.

C. maintaining the disaster recovery plan.

D. reviewing the disaster recovery requirements of supplier contracts.

4-9

Data mirroring should be implemented as a recovery strategy when: A. recovery point objective (RPO) is low.

B. recovery point objective (RPO) is high.

C. recovery time objective (RTO) is high.

D. disaster tolerance is high.

4-10 Which of the following components of a business continuity plan is **PRIMARILY** the responsibility of an organization's IS department?

A. Developing the business continuity plan

B. Selecting and approving the recovery strategies used in the business continuity plan

C. Declaring a disaster

D. Restoring the IT systems and data after a disaster

ANSWERS TO SELF-ASSESSMENT QUESTIONS

4-1

A.

User satisfaction is the measure to ensure that an effective

information processing operation meets user requirements.

B.

Goal accomplishment evaluates effectiveness involved in

comparing performance with predefined goals.

C.

Benchmarking provides a means of determining the level of

performance offered by similar information processing

facility environments.

D.

Capacity and growth planning are essential due to the importance of IT in

organizations and the constant change in technology.

4-2

A.

Mobile sites are specially designed trailers that can be quickly transported to a business location or to an alternate site to provide a ready-conditioned information processing facility (IPF).

B.

Warm sites are partially configured, usually with network

connections and selected peripheral equipment—such as disk

drives, tape drives and controllers—but without the main

computer.

C.

Cold sites have only the basic environment to operate an IPF.

Cold sites are ready to receive equipment, but do not offer any

components at the site in advance of the need.

D.

Hot sites are fully configured and ready to operate within

several hours or, in some cases, even minutes.

4-3

A.

When testing change management, the IS auditor should

always start with system-generated information, containing

the date and time a module was last updated, and trace from

there to the documentation authorizing the change.

B.

Focusing exclusively on the accuracy of the documentation

examined does not ensure that all changes were, in fact,

documented.

C.

To trace in the opposite direction would run the risk of not

detecting undocumented changes.

D.

Focusing exclusively on the completeness of the documentation

examined does not ensure that all changes were, in fact,

documented.

4-4

A.

Virtual private network (VPN) technology allows external

partners to securely participate in the extranet using public networks as a transport or shared private network. Because

of low cost, using public networks (Internet) as a transport is the principal method. VPNs rely on tunneling/encapsulation

techniques, which allow the Internet Protocol (IP) to carry a variety of different protocols (e.g., SNA and IPX).

B.

Client-server does not address extending the network to business partners (i.e., client-servers refers to a group of computers within an organization connected by a communications network where

the client is the requesting machine and the server is the

supplying machine).

C.

Although it may be technically possible for an enterprise to

extend its intranet using dial-up access, it would not be practical or cost effective to do so.

D.

A network service provider may provide services to a shared

private network by providing Internet services, but it does not

extend an organization’s intranet.

4-5

A.

The criticality classification is determined by the role of the application system in supporting the strategy of the organization.

B.

The replacement cost of the application does not reflect the

relative value of the application to the business.

C.

Vendor support is not a relevant factor for determining the

criticality classification.

D.

The associated threats and vulnerabilities will get evaluated only if the application is critical to the business.

4-6

A.

System utilities may enable unauthorized changes to be made

to data on the client-server database. In an audit of database security, the controls over such utilities would be the primary concern of the IS auditor.

B.

Application program generators are an intrinsic part of client-

server technology, and the IS auditor would evaluate the controls over the generators access rights to the database rather than their availability.

C.

Security documentation should be restricted to authorized

security staff, but this is not a primary concern.

D.

Access to stored procedures is not a primary concern.

4-7

A.

Reviewing validity of password changes would be performed as

part of substantive testing.

B.

Understanding the network architecture and design is the starting point for identifying the various layers of information and the

access architecture across the various layers, such as client-server applications.

C.

The first step in auditing a network is to understand the

network architecture and design. Understanding the network

architecture and design provides an overall picture of the

network and its connectivity.

D.

Understanding the network architecture and design is the starting point for identifying the various layers of information and the

access architecture across the various layers, such as proxy

servers and firewalls.

4-8

A.

The IS auditor should always be present when disaster

recovery plans are tested to ensure that the tested recovery

procedures meet the required targets for restoration, that

recovery procedures are effective and efficient, and to report on the results, as appropriate.

B.

IS auditors may be involved in overseeing plan development, but they are unlikely to be involved in the actual development process.

C.

Similarly, an audit of plan maintenance procedures may be conducted, but the IS auditor normally would not have any responsibility for the actual maintenance.

D.

An IS auditor may be asked to comment upon various elements of a supplier contract, but, again, this is not always the case.

4-9

A.

Recovery point objective (RPO) is the earliest point in time at which it is acceptable to recover the data. In other words, RPO indicates the age of the recovered data (i.e., how long ago the data were backed up or otherwise replicated). If RPO is very low, such as minutes, it means that the organization cannot afford to lose even a few minutes of data. In such cases, data mirroring (synchronous data replication) should be used as a recovery strategy.

B.

If RPO is high, such as hours, then other backup procedures—

such as tape backup and recovery—could be used.

C.

A high recovery time objective (RTO) means that the IT system

may not be needed immediately after the disaster

declaration/disruption (i.e., it can be recovered later).

D.

RTO is the time from the disruption/declaration of disaster during which the business can tolerate nonavailability of IT facilities. If RTO is high, slower recovery strategies that bring up IT systems and facilities can be used.

4-10 A.

Members of the organization’s senior management are primarily

responsible for overseeing the development of the business

continuity plan for an organization and are accountable for the

results.

B.

Management is also accountable for selecting and approving the

strategies used for disaster recovery.

C.

IT may be involved in declaring a disaster but is not primarily

responsible.

D.

The correct choice is restoring the IT systems and data after a disaster. The IT department of an organization is primarily

responsible for restoring the IT systems and data after a

disaster within the designated timeframes.

PART A: INFORMATION SYSTEMS

OPERATIONS

4.0 INTRODUCTION

IT service management practices are important to provide assurance to users and to management that the expected level of service will be delivered.

Service level expectations are derived from the organization's business objectives. IT service delivery includes IS operations, IT services, and management of IS and the groups responsible for supporting them. IT

services are built on service management frameworks.

4.1 COMMON TECHNOLOGY COMPONENTS

This section introduces:

• Technology components

• Hardware platforms

• Basic concepts of, and history behind, the different types of computers

• Advances in IT

Also discussed are the key audit considerations, such as capacity management, system monitoring, maintenance of hardware and typical steps in the acquisition of new hardware.

Note: Vendor-specific terminology is used within this manual for illustrative purposes only. Candidates will not be examined on the components of vendor-specific hardware offerings or on vendor-specific terminology unless this

terminology has become generalized and is used globally.

4.1.1 COMPUTER HARDWARE COMPONENTS AND ARCHITECTURES

Computer-system hardware components are interdependent components that perform specific functions and can be classified as either processing or input/output.

Processing Components

The central component of a computer is the central processing unit (CPU).

Computers may:

• Have the CPU on a single chip (microprocessors)

• Have more than one CPU (multi-processor)

• Contain multiple CPUs on a single chip (multi-core processors) The CPU consists of an arithmetic logic unit (ALU), a control unit and an internal memory. The control unit contains electrical circuits that control/direct all operations in the computer system. The ALU performs mathematical and logical operations. The internal memory (i.e., CPU

registers) is used for processing transactions.

Other key components of a computer include:

• Motherboard

• Random access memory (RAM)

• Read-only memory (ROM)

• Permanent storage devices (hard disk drive or solid-state drive [SSD])

• A power supply unity

An SSD is nonvolatile storage device that stores persistent data on solid-state

flash memory. SSDs have no moving components and, therefore, require less energy. This distinguishes them from hard disk drives, which contain spinning disks and movable read/write heads.

Input/Output Components

The input/output (I/O) components are used to pass instructions/information to the computer and to display or record the output generated by the computer. Some components, such as the keyboard and mouse, are input-only devices, while others, such as the touch screen, are both input and output devices. Printers are an example of an output-only device.

Types of Computers

Computers can be categorized according to several criteria—mainly their

processing power, size and architecture. These categories are shown in **figure**

4.1.

4.1.2 COMMON ENTERPRISE BACK-END DEVICES

In a distributed environment, many different devices are used to deliver application services. One factor that has significantly changed in recent years is the rapid growth of the Internet of Things (IoT). Organizations need to know and embrace the many connected items in use, including cars, thermostats, video cameras, mattresses and medical equipment, and understand how they are affecting operations. Although increased innovation, productivity and services offer benefits, IoT use also risks data leakage and privacy issues, among others. See chapter 5, Protection of Information Assets, for more information.

Following are some of the most common devices encountered:

• **Print servers**—Businesses of all sizes require that printing capability be made available to users across multiple sites and domains. Generally, a network printer is configured based on where the printer is physically located and who within the organization needs to use it. Print servers allow businesses to consolidate printing resources for cost savings.

• **File servers**—File servers provide for organizationwide access to files and

programs. Document repositories can be centralized to a few locations within the organization and controlled with an access-control matrix.

Group collaboration and document management are easier when a

document repository is used, rather than dispersed storage across multiple workstations.

• **Application (program) servers**—Application servers typically host the software programs that provide application access to client computers, including processing the application business logic and communication with the application's database. Consolidation of applications and licenses in servers enables centralized management and a more secure environment.

• **Web servers**—Web servers provide information and services to external customers and internal employees through web pages. They are normally

accessed by their uniform resource locators (URLs).

Figure 4.1—Common Types of Computers

Supercomputers

Very large and expensive computers with the highest processing speed, designed to be used for specialized purposes or fields that require extensive processing power (e.g., complex mathematical or logical calculations). They are typically dedicated to a few specific specialized system or application programs.

Mainframes

Large, general-purpose computers that are made to share their processing power and facilities with thousands of internal or external users. Mainframes accomplish this by executing a large variety of tasks almost simultaneously. The range of capabilities of these computers is extensive. A mainframe computer often has its own proprietary OS that can support background (batch) and real-time (online) programs operating parallel applications. Mainframes have traditionally been the main data processing and data warehousing resource of large organizations and, as such, have long been protected by a number of the early security and control tools.

High-end and

Multiprocessing systems capable of supporting thousands of simultaneous midrange servers

users. In size and power, they can be comparable to a mainframe. High-end/midrange servers have many of the control features of mainframes such as online memory and CPU management, physical and logical partitioning, etc.

Their capabilities are also comparable to mainframes in terms of speed for processing data and execution of client programs, but they cost much less than mainframes. Their OSs and system software base components are often commercial products. The higher-end devices generally use UNIX and, in many cases, are used as database servers while smaller devices are more likely to utilize the Windows OS and be used as application servers and file/print servers.

Personal

Small computer systems referred to as PCs or workstations that are designed for computers (PCs)

individual users, inexpensively priced and based on microprocessor technology.

Their use includes office automation functions such as word processing, spreadsheets and email; small database management; interaction with web-based applications; and others such as personal graphics, voice, imaging, design, web access and entertainment. Although designed as single-user systems, these computers are commonly linked together to form a network.

Thin client

These are personal computers that are generally configured with minimal computers

hardware features (e.g., diskless workstation) with the intent being that most processing occurs at the server level using software, such as Microsoft Terminal Services or Citrix Presentation Server, to access a suite of applications.

Laptop computers

Lightweight (under 10 pounds/5 kilograms) personal computers that are easily transportable and are powered by a normal AC connection or by a rechargeable battery pack. Similar to the desktop variety of personal computers in capability, they have similar CPUs, memory capacity and disk storage capacity, but the battery pack makes them less vulnerable to power failures.

Being portable, these are vulnerable to theft. Devices may be stolen to obtain information contained therein and hijack connectivity, either within an internal local area network (LAN) or remotely.

Smartphones,

Handheld devices that enable their users to use a small computing device as a tablets and other

substitute for a laptop computer. Some of its uses include a scheduler, a handheld devices

telephone and address book, creating and tracking to-do lists, an expense manager, eReader, web browser, and an assortment of other functions. Such devices can also combine computing, telephone/fax and networking features together so they can be used anytime and anywhere. Handheld devices are also capable of interfacing with PCs to back up or transfer important information.

Likewise, information from a PC can be downloaded to a handheld device.

• **Proxy servers**—Proxy servers provide an intermediate link between users and resources. As opposed to direct access, proxy servers will access services on a user's behalf. Depending on the services being proxied, a proxy server may render more secure and faster response than direct access.

• **Database servers**—Database servers store data and act as a repository. The servers concentrate on storing information rather than presenting it to be usable. Application servers and web servers use the data stored in database servers and process the data into usable information.

• **Appliances (specialized devices)**—Appliances provide a specific service and normally are not capable of running other services. As a result, the devices are significantly smaller and faster, and very efficient. Capacity and performance demands require certain services to be run on appliances instead of generic

servers. Examples of appliances are:

– Firewalls

– Intrusion detection systems (IDSs)

– Intrusion prevention systems (IPSs)

– Switches

– Routers

– Virtual private networks (VPNs)

– Load balancers

Note: See chapter 5, Protection of Information Assets, for more information on these appliances.

4.1.3 UNIVERSAL SERIAL BUS

The universal serial bus (USB) is a serial bus standard that interfaces devices with a host. USB was designed to allow connection of many peripherals to a single standardized interface socket and to improve the plug-and-play capabilities by allowing hot swapping or allowing devices to be connected and disconnected without rebooting the computer or turning off the device.

Other convenient features include providing power to low-consumption devices without the need for an external power supply and allowing many devices to be used without requiring installation of manufacturer-specific, individual device drivers.

USB ports overcome the limitations of the serial and parallel ports in terms of speed and the actual number of connections that can be made. USB 2.0

specifications support data transfer at up to 480 megabits per second (Mbps).

USB 3.0 can transfer data at up to ten times that speed, five gigabits per second (Gbps), and the latest version USB3.1 is capable of transfer speeds up to 10 Gbps.

USB ports can connect computer peripherals, such as mice, keyboards, tablets, gamepads, joysticks, scanners, digital cameras, printers, personal media players, flash drives and external hard drives. Most operating systems (OSs) recognize when a USB device is connected and load the necessary device drivers.

A **memory card** or **flash drive** is a solid-state electronic data storage device that is used with digital cameras, handheld and mobile computers, telephones, music players, video game consoles and other electronics. They offer high recordability, power-free storage, a small form factor and rugged environmental specifications. Examples include Memory Stick,

CompactFlash, SD (secure digital) and flash drive.

Risk Related to USBs

Risk related to the use of USBs includes the following:

• **Viruses and other malicious software**—USB drives present a vector for computer viruses that is very difficult to defend against. Whenever files are transferred between two machines, there is a risk that malware (e.g.,

viruses, spyware and keyloggers) will be transmitted, and USB drives are no exception. Some USB drives include a physical switch that can put the drive in read-only mode. When transferring files to an untrusted machine, a USB drive that is in read-only mode will prevent any data (including viruses) to be written to the device.

• **Data theft**—Hackers, corporate spies and disgruntled employees steal data, and in many cases, these are crimes of opportunity. With a USB drive, any unattended and unlocked PC with a USB port provides an opportunity for criminal activity. Social engineering can give a hacker physical access to a corporate PC to steal data or plant spyware.

• **Data and media loss**—The portability of USB drives presents an increased risk for lost data and media. If an unencrypted USB device is lost, any individual who finds the device will be able to access the data on the drive.

• **Corruption of data**—If the drive is improperly unplugged, then data loss can occur due to corruption. USB drives differ from other types of removable media, such as CD-ROM and DVD-ROM devices, because the computer is not

automatically alerted when USB drives are removed. Users of USB drives must alert the computer when they intend to remove the device; otherwise, the computer will be unable to perform the necessary clean-up functions required to disconnect the device, especially if files from the device are currently open.

• **Loss of confidentiality**—Because of its convenient small physical size and large logical size, a significant amount of data can be stored on a USB

drive. Some stored information is confidential, and loss of data becomes a risk when the drive is lost, increasing the risk of the data falling into the hands of a competitor. Legal issues can also be associated with loss of confidentiality. For example, in the United States, lost or compromised patient data can indicate a breach of patient privacy, thus violating the Health Insurance Portability and Accountability Act (HIPAA).

Security Controls Related to USBs

The following controls can be used to help reduce risk associated with the use of USB devices:

• **Encryption**—An ideal encryption strategy allows data to be stored on the USB drive but renders the data useless without the required encryption key, such as a strong password or biometric data. Products are available to

implement strong encryption and comply with the latest Federal Information Processing Standards (FIPS). Encryption is a good method to protect information written to the device from loss or theft of the device.

But unless the information is also encrypted on the network or local workstation hard drive, sensitive data still are exposed to theft.

• **Granular control**—Products are available to provide centralized management of ports. Because management is accomplished via the use of specialized software, centralized management from the enterprise to the individual system is possible. As with all security issues, a technological solution in isolation is insufficient. Strong policies, procedures, standards and guidelines must be put in place to ensure secure operation of memory card and USB drives. Further, an aggressive user awareness program is necessary to effect changes in employee behavior.

• **Security personnel education**—Flash drives are so small and unobtrusive that they are easily concealed and removed from an enterprise. Physical security personnel should understand USB devices and the risk they present.

• **The lock desktop policy enforcement**—In higher-risk environments, desktop computers should be configured to automatically lock after short intervals.

• **Antivirus policy**—Antivirus software should be configured to scan all attached drives and removable media. Users should be trained to scan files before opening them.

• **Use of secure devices only**—Enforce the use of encryption. Software is available to manage USBs, enforcing encryption or only accepting encrypted devices.

• **Inclusion of return information**—If a USB drive is lost or misplaced, including a small, readable text file containing return information may help with device retrieval. It would be prudent to NOT include company details, but rather a phone number or post office box. It also would be prudent to include a legal disclaimer that clearly identifies the information on the drive as confidential and protected by law.

4.1.4 RADIO FREQUENCY IDENTIFICATION

Radio frequency identification (RFID) uses radio waves to identify tagged

objects within a limited radius. A tag consists of a microchip and an antenna.

The microchip stores information along with an ID to identify a product, while the antenna transmits the information to an RFID reader.

The power needed to drive the tag can be derived in two modes. The first mode, used in passive tags, draws power from the incidental radiation arriving from the reader. The second and more expensive mode, used in active tags, derives its power from batteries and therefore is capable of using higher frequencies and achieving longer communication distances. An active tag is reusable and can contain more data.

Tags can be used to identify an item based on either direct product identification or carrier identification. In the case of the latter, an article’s ID

is manually fed into the system (e.g., using a bar code) and is used along with strategically placed radio frequency readers to track and locate the item.

Applications of RFID

Application of RFID include the following:

• **Asset management**—RFID-based asset management systems are used to manage inventory of any item that can be tagged. Asset management systems using RFID technology offer significant advantages over paper-based or bar-code systems, including the ability to read the identifiers of multiple items nearly simultaneously without optical line of sight or physical contact.

• **Tracking**—RFID asset management systems are used to identify the location of an item or, more accurately, the location of the last reader that detected the presence of the tag associated with the item.

• **Authenticity verification**—The tag provides evidence of the source of a tagged item. Authenticity verification often is incorporated into a tracking application.

• **Matching**—Two tagged items are matched with each other and a signal (e.g., a light or tone) is triggered if one of the items is later matched with an incorrect tagged item.

• **Process control**—This allows business processes to use information associated with a tag (or the item attached to the tag) and to take a customized action.

• **Access control**—The system uses RFID to automatically check whether an individual is authorized to physically access a facility (e.g., a gated campus or a specific building) or logically access an information technology system.

• **Supply chain management (SCM)**—SCM involves the monitoring and control of products from manufacture to distribution to retail sale. SCM

typically bundles several application types, including asset management, tracking, process control and payment systems.

Risk Associated With RFID

Some of the risk associated with RFID includes:

• **Business process risk**—Direct attacks on RFID system components can undermine the business processes that the RFID system was designed to enable.

• **Business intelligence risk**—An adversary or competitor can gain unauthorized access to RFID-generated information and use the

information to harm the interests of the organization implementing the RFID system.

• **Privacy risk**—Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because possession can enable tracking of those tagged items.

• **Externality risk**—RFID technology can represent a threat to non-RFID-networked or non-RFID-collocated systems, assets and people. An

important characteristic of RFID that impacts the risk is that RF

communication is invisible to operators and users.

Security Controls for RFID

Some security controls for RFID include:

• **Management**—A management control involves oversight of the security of the RFID system. For example, management staff of an organization may need to update existing policies to address RFID implementations, such as security controls needed for an RF subsystem.

• **Operational**—An operational control involves the actions performed on a daily basis by the system's administrators and users. For example, RFID

systems need operational controls that ensure the physical security of the systems and their correct use.

• **Technical**—A technical control uses technology to monitor or restrict the

actions that can be performed within the system. RFID systems need technical controls for several reasons, such as protecting or encrypting data on tags, causing tags to self-destruct and protecting or encrypting wireless communications.

4.1.5 HARDWARE MAINTENANCE PROGRAM

To ensure proper operation, hardware must be routinely cleaned and serviced.

Maintenance requirements vary based on complexity and performance workloads (e.g., processing requirements, terminal access and number of applications running). Maintenance should be scheduled to closely coincide with vendor-provided specifications. Maintenance is also important for environmental hardware that controls temperature and humidity, fire protection and electrical power. The hardware maintenance program is designed to document the performance of this maintenance.

Information typically maintained by this program includes:

• Reputable service company information for each hardware resource requiring routine maintenance

• Maintenance schedule information

• Maintenance cost information

• Maintenance performance history information, such as planned versus unplanned, executed and exceptional

IS management should monitor, identify and document any deviations from vendor maintenance specifications and provide supporting arguments for this deviation.

When performing an audit of this area, the IS auditor should:

• Ensure that a formal maintenance plan has been developed and approved by management and is being followed.

• Identify maintenance costs that exceed budget or are excessive. These overages may be an indication of a lack of adherence to maintenance procedures or of

upcoming changes to hardware. Proper inquiry and

follow-up procedures should be performed.

Hardware Monitoring Procedures

The following are typical procedures and reports for monitoring the effective and efficient use of hardware:

• **Availability reports**—These reports indicate the time periods during which the computer is in operation and available for use by users or other processes. A key concern addressed by this report is excessive IS

unavailability, referred to as downtime. This unavailability may indicate inadequate hardware facilities, excessive OS maintenance, the need for preventive maintenance, inadequate environmental facilities (e.g., power supply or air conditioning) or inadequate training for operators.

• **Hardware error reports**—These reports identify CPU, I/O, power and storage failures. These reports should be reviewed by IS operations management to ensure that equipment is functioning properly, to detect failures and to initiate corrective action. The IS auditor should be aware that attribution of an error in hardware or software is not necessarily easy and immediate. Reports should be checked for intermittent or recurring problems, which might indicate difficulties in properly diagnosing the errors.

• **Asset management reports**—These reports provide an inventory of network-connected equipment, such as PCs, servers, routers and other devices.

• **Utilization reports**—These automated reports document the use of the machine and peripherals. Software monitors are used to capture utilization measurements for processors, channels and secondary storage media, such as disk and tape drives. Depending on the OS, resource utilization for multiuser computing environments found in mainframe/large-scale

computers should average in the 85- to 95-percent range, with allowances for utilization occasionally reaching 100 percent and falling below 70

percent. Trends from utilization reports can be used by IS management to predict whether more or fewer processing resources are required.

4.1.6 HARDWARE REVIEWS

When auditing infrastructure and operations, hardware reviews should

include the areas shown in **figure 4.2**.

4.2 IT ASSET MANAGEMENT

An asset is something of either tangible or intangible value that is worth protecting and includes people, information, infrastructure, finances and reputation. However, an asset cannot be effectively protected or managed if it is not identified. Likewise, it makes it more difficult to protect an asset if its location is unknown or no owner is assigned.

Figure 4.2—Hardware Reviews

Areas to Review	Questions to Consider
Hardware acquisition plan	• Is the plan aligned with business requirements? • Is the plan aligned with the enterprise architecture? • Is the plan compared regularly to business plans to ensure continued synchronization with business requirements? • Is the plan synchronized with IS plans? • Have criteria for the acquisition of hardware been developed? • Is the environment adequate to accommodate the currently installed hardware and new hardware to be added under the approved hardware acquisition plan? • Are the hardware and software specifications, installation requirements and the likely lead time associated with planned acquisitions adequately documented?
Acquisition of hardware	• Is the acquisition in line with the hardware acquisition plan? • Have the IS management staff issued written policy statements regarding the acquisition and use of hardware, and have these statements been communicated to the users?

• Have procedures and forms been established to facilitate the

acquisition approval process?

• Are requests accompanied by a cost-benefit analysis?

• Are purchases routed through the purchasing department to

streamline the process, avoid duplications, ensure compliance with tendering requirements and legislation and to take advantage of

quantity and quality benefits such as volume discounts?

IT asset management

• Has the hardware been tagged?

• Has an owner been designated?

• Where will the hardware be located?

• Have we retained a copy of the contracts/SLAs?

Capacity management and

• Are criteria used in the hardware performance monitoring plan

monitoring

based on historical data and analysis obtained from the IS trouble

logs, processing schedules, job accounting system reports, preventive maintenance schedules and reports?

• Is continuous review performed of hardware and system software performance and capacity?

• Is monitoring adequate for equipment that has been programmed to contact its manufacturer (without manual or human intervention) in the case of equipment failure?

Preventive maintenance

• Is the prescribed maintenance frequency recommended by the

schedule

respective hardware vendors being observed?

• Is maintenance performed during off-peak workload periods?

• Is preventive maintenance performed at times other than when the system is processing critical or sensitive applications?

Hardware availability and

• Is scheduling adequate to meet workload schedules and user

utilization reports

requirements?

• Is scheduling sufficiently flexible to accommodate required

hardware preventive maintenance?

• Are IS resources readily available for critical application programs?

Problem logs Job

• Have IS management staff reviewed hardware malfunctions,

accounting system reports

reruns, abnormal system terminations and operator actions?

The first step in IT asset management is the process of identifying and creating an inventory of IT assets. The inventory record of each information asset should include:

• Owner

• Designated custodian

• Specific identification of the asset

• Relative value to the organization

• Loss implications and recovery priority

• Location

• Security/risk classification

• Asset group (where the asset forms part of a larger information system)
Common methods to build the initial inventory include consulting the purchasing system, reviewing contracts and reviewing the software currently installed, using tools, such as Microsoft® System Center Configuration Manager, Spiceworks and ManageEngine.

IT asset management is a fundamental prerequisite to developing a meaningful security strategy. Developing a list of assets is the first step in

managing software licenses (see section 4.7.6, Software Licensing Issues) and classifying and protecting information assets (see section 5.1, Information Asset Security Frameworks, Standards and Guidelines).

IT asset management should be employed for software and hardware assets.

It is common to physically tag hardware assets.

4.3 JOB SCHEDULING AND PRODUCTION PROCESS AUTOMATION

In complex IS environments, computer systems transfer hundreds to thousands of data files daily. A job schedule is typically created that lists the jobs that must be run and the order in which they are run, including any dependencies. Due to the inherent complexity of this process, automated job scheduling software provides control over the scheduling process. In addition to the scheduling of batch jobs, job scheduling software can be used to schedule tape backups and other maintenance activities. Job scheduling is a major function within the IT

department. The schedule includes the jobs that must be run, the sequence of job execution and the conditions that cause program execution. Low-priority jobs can also be scheduled, if time becomes available.

High-priority jobs should be given optimal resource availability, and maintenance functions (such as backup and system reorganization) should, if possible, be performed during nonpeak times. Schedules provide a means of keeping customer demand at a manageable level and permit unexpected or on-request jobs to be processed without unnecessary delay.

Job scheduling procedures are necessary to ensure that IS resources are used optimally, based on processing requirements. Applications are increasingly required to be continually available; therefore, job scheduling (maintenance or long processing times) represents a greater challenge than before.

4.3.1 JOB SCHEDULING SOFTWARE

Job scheduling software is system software used by installations that process a large number of batch routines. The scheduling software sets up daily work

schedules and automatically determines which jobs are to be submitted to the system for processing.

The advantages of using job scheduling software include:

• Job information is set up only once, reducing the probability of an error.

• Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.

• Records are maintained of all job successes and failures.

• Security over access to production data can be provided.

• Reliance on operators is reduced.

4.3.2 SCHEDULING REVIEWS

Figure 4.3 describes an audit approach to be considered when reviewing workload job scheduling and personnel scheduling.

Figure 4.3—Scheduling Reviews

Areas to Review	Questions to Consider
• Regularly scheduled	
• Are the items included in SLAs?	
applications	
• Are the items functioning according to the SLAs?	
• Input deadlines	
• Data preparation time	
• Estimated processing time	
• Output deadlines	
• Procedures for collecting,	
reporting and analyzing	
key performance	
indicators	
• Job schedule	
• Have critical applications been identified and the highest priority assigned to them?	
• Have processing priorities been established for other applications and are the assigned priorities justified?	
• Is scheduling of rush/rerun jobs consistent with their assigned priority?	
• Do scheduling procedures facilitate optimal use of computer	

resources while meeting service requirements?

• Do operators record jobs that are to be processed and the required data files?

• Do operators schedule jobs for processing on a predetermined basis and perform them using either automated scheduling software or a manual schedule?

• Daily job schedule

• Is the number of personnel assigned to each shift adequate to

support the workload?

• Does the daily job schedule serve as an audit trail? Does the

schedule provide each shift of computer operators with the work to be carried out, the sequence in which programs are to be run and indication when lower-priority work can be performed?

• At the end of a shift, does each operator pass to the work scheduler or the next shift of operators a statement of the work completed and the reasons any scheduled work was not finished?

• Console log

• Were jobs run and completed according to the schedule?

• If not, are the reasons valid?

• Exception processing logs

• Do operators obtain written or electronic approval from owners when scheduling request-only jobs?

• Do operators record all exception processing requests?

• Do operators review the exception processing request log to

determine the appropriateness of procedures performed?

• Reexecuted jobs

• Are all reexecution of jobs properly authorized and logged for IS

management review?

• Are procedures established for rerunning jobs to ensure that the correct input files are being used and subsequent jobs in the

sequence also are rerun, if appropriate?

• Personnel

• Are personnel who are capable of assigning, changing job

schedules or job priorities authorized to do so?

4.4 SYSTEM INTERFACES

A system is a set of elements, including hardware and software, that work together to run one or more computers. System interfaces exist where data output from one application is sent as input to another, with little or no human interaction. Interfaces that involve humans are usually called user interfaces.

System interfaces provide the ability to transfer data even if the systems use different programming languages or were created by different developers.

This offers organizations a greater level of flexibility to choose the applications that best serve different areas, even if those areas need to share data.

Generally, data transfers through system interfaces can be sorted into three categories: system-to-system, partner-to-partner and person-to-person.

System-to-system interfaces occur when data is transferred between two systems, whether internal or external. Data may also be transferred to specialized tools for analysis. These uses have increased in part because of the growing popularity of business analytics, which involves transferring data from a repository to an analytic tool to obtain intelligence and insights via data mining.

Partner-to-partner interface occurs when two partners are continuously transferring data back and forth across agreed-upon systems. These transfers are generally done on a regular basis.

Person-to-person transfers are often the most unnoticed and unmanaged.

They can be as easy as attaching a data file to an email and sending it. These forms of transfer tend to be more difficult to observe, manage, secure and control.

4.4.1 RISK ASSOCIATED WITH SYSTEM INTERFACES

Recognizing this growth, organizations are focusing more on ensuring that there is a centralized methodology for tracking and managing system interfaces and that there are documentation and audit trails for relevant government regulations. Unmanaged interfaces can add to the risk regarding data security, privacy and error.

It is critical that organizations are able to rely on the integrity of the data exchanged through system interfaces. If an interface is not functioning correctly, one possible consequence is that incorrect management reports (e.g., research, financial, intelligence, performance and competitive) have a significant negative impact on a business and decision-making. Beyond an effect on business value, even a small error can invoke potential legal compliance liability.

4.4.2 SECURITY ISSUES IN SYSTEM INTERFACES

The primary objective of maintaining security of data being transferred through system interfaces is to ensure that the data intended to be extracted from the originating system are the same as the data that were downloaded and recorded in the recipient system. The data need to be protected and

secured throughout the transfer process. The secondary objective is to prevent unauthorized access to the data via interception, malicious activity, error or other means. Unavailability of system interfaces can also affect the reliability of data.

4.4.3 CONTROLS ASSOCIATED WITH SYSTEM

INTERFACES

The IS auditor should ensure that the organization has a program that tracks and manages all system interfaces and data transfers, whether internal or external, in line with the business needs and goals. This includes the ability to see all the transfers made, including those that are ad hoc, whether the organization is using

a commercial or custom managed file transfer (MFT) system. IS auditors should ensure that the program is able to:

• Manage multiple file transfer mechanisms.

• Use multiple protocols.

• Automatically encrypt, decrypt and electronically sign data files.

• Compress/decompress data files.

• Connect to common database servers.

• Send and retrieve files via email and secure email.

• Automatically schedule regular data transfers.

• Analyze, track and report any attributes of the data being transferred.

• Ensure compliance with appropriate regulatory laws and mandates.

• Offer a checkpoint or restart capability for interruptions.

• Integrate with back-office applications to automate data transfers as much as feasible.

Controls need to be implemented with the objective of ensuring that the data residing on the sending system are precisely the same data that are recorded on the receiving system. For example, an organization may use a software package that can generate controls during the extraction that automatically reconcile the data after they are recorded on the receiving system.

Although automated controls are generally preferred over manual controls, another control can be manual reconciliation by running a report of the data sent and comparing it to a report on the data received. This should be done by

a qualified person who has the ability to detect material differences in the data.

IS auditors should also ascertain if the organization is using encryption, as appropriate for each use, to protect data during the transfer. Encryption is necessary when the risk of unauthorized access or interception is relatively high

(e.g., industrial espionage, identity theft, credit card data theft).

Additionally, the transfer process may require strong access and authentication controls, and the data files might be password-protected.

There also should be a control over nonrepudiation, which ensures that the intended recipient is the actual recipient of the data.

To ensure that an audit trail is associated with the system interface, the organization needs to capture important information, including who sent the data, when they were sent, when they were received, what data structure (e.g., xls, csv, txt or xml) was used, how the data were sent and who received the data. This includes assessing automated logs of servers along the path, especially if the data are transmitted to an external system where they touch multiple Internet hosts and are more exposed to hackers and cybercriminals.

4.5 END-USER COMPUTING

End users are the people who access business applications that were programmed, serviced and installed by others. End-user computing (EUC) refers to the ability of end users (who typically are not programmers) to design and implement their own application or information system using computer software products. Often, an end-user support manager is a liaison between an IT department and end users.

One of the benefits of EUC is that users can quickly build and deploy applications, taking the pressure off of the IT department. EUC also enables organizations to be more flexible and more rapidly address shifting marketplaces, regulations and consumer interests.

Lack of IT department involvement in EUC also brings associated risk, because the applications may not be subject to an independent review and,

frequently, are not created in the context of a formal development methodology.

This lack of IT department involvement can result in applications that:

• May contain errors and give incorrect results

• Are not subject to change management or release management, resulting in

multiple, perhaps different, copies

• Are not secured

• Are not backed up

The lack of IT department oversight of EUC can lead to security risk.

Examples include:

• **Authorization**—There may be no secure mechanism to authorize access to the system.

• **Authentication**—There may be no secure mechanism to authenticate users to the system.

• **Audit logging**—This is not available on standard EUC solutions (e.g., Microsoft Excel and Access).

• **Encryption**—The application may contain sensitive data which have not been encrypted or otherwise protected.

In most instances, EUC applications do not pose a significant risk to the enterprise. Nonetheless, management should define risk criteria to determine the criticality of the application. These applications should also be subject to data classification, and those deemed critical enough should be subject to the same controls as any other application.

Organizations need to manage and control EUC and the IS auditor should ensure that policies for the use of EUC exist. An inventory (see section 4.2, IT Asset Management) of all such applications should exist, and those deemed critical enough should be subject to the same controls as any other application.

4.6 DATA GOVERNANCE

With ever-changing data environments—such as the cloud—and data

requirements, data maintenance and management are becoming increasingly

complicated. Data also exists in many forms, such as text, numbers, graphics and

video. After data are made meaningful, they become information, which is crucial to the operation of an enterprise.

Data governance ensures that:

• Stakeholder needs, conditions and options are evaluated to determine balanced, mutually agreed enterprise objectives to be achieved through the acquisition and management of data/information resources.

• Direction is set for data/information management capabilities through prioritization and decision making.

• Performance and compliance of data/information resources are monitored and evaluated relative to mutually agreed-upon (by all stakeholders) direction and objectives.

Data governance reflects the practice of evaluating requirements and bringing direction and control over data and information so that users have access to that data and can trust and rely on it.

Data governance also involves monitoring the performance of IT operations, specifically those areas that relate to data and its availability, integrity and confidentiality.

4.6.1 DATA MANAGEMENT

The *Data Management Body of Knowledge* (DMBOK) defines data management as “the planning and execution of policies, practices, and projects that acquire, control, protect, deliver, and enhance the value of data and information assets.”

Data management is a component of data architecture, which is a key part of enterprise architecture.

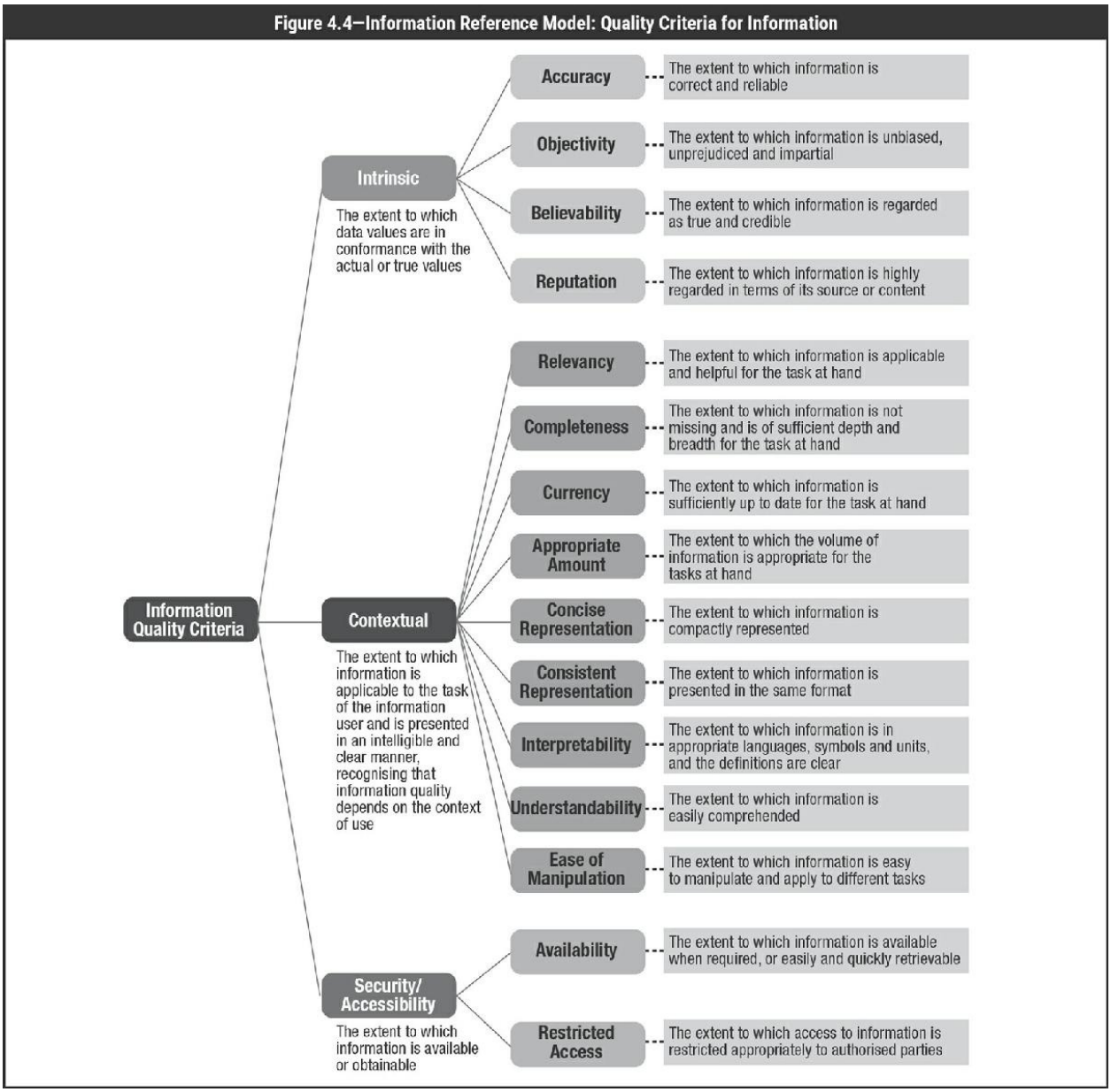
Data Quality

Data quality is key to data management. There are three subdimensions of quality: intrinsic, contextual and security/accessibility. Each subdimension is divided further into several quality criteria, which are defined in **figure 4.4.**

Data Life Cycle

A life cycle describes a series of stages that characterize the course of existence of an organizational investment. Data life cycle management describes the stages that data go through in the course of existence in an organization. The data life cycle includes the following elements:

• **Plan**—The phase in which the creation, acquisition and use of the information resource is prepared. Activities in this phase include understanding information use in the respective business processes, determining the value of the information asset and its associated classification, identifying objectives and planning the information architecture.



Source: ISACA, *COBIT 2019 Framework: Introduction and Methodology*, USA, 2018.

• **Design**—The phase in which more detailed work is done in specifying how the information will look and how systems processing the information will have to work. Activities in this phase may refer to the development of standards and definitions (e.g., data definitions, data collection, access, storage procedures, metadata characteristics and data classification).

• **Build/acquire**—The phase in which the information resource is acquired.

Activities in this phase may refer to the creation of data records, the purchase of data and the loading of external files.

• **Use/operate**—This phase includes:

– Store—The phase in which information is held electronically or in hard copy (or even just in human memory). Activities in this phase may refer to the storage of information in electronic form (e.g., electronic files, databases and data warehouses) or as hard copy (e.g., paper documents).

– Share—The phase in which information is made available for use through a distribution method. Activities in this phase may refer to the processes involved in getting the information to places where it can be accessed and used (e.g., distributing documents by email). For

electronically held information, this life cycle phase may largely overlap with the store phase (e.g., sharing information through database access and file/document servers).

– Use—The phase in which information is used to accomplish (IT-related and thus enterprise) goals. Activities in this phase may refer to all kinds of information usage (e.g., managerial decision making and running automated processes) and include activities, such as information retrieval and converting information from one form to another.

Information use as defined in the information model can be thought of as the purposes for which enterprise stakeholders need information when assuming their roles, fulfilling their activities and interacting with each other.

• **Monitor**—The phase in which it is ensured that the information resource continues to work properly (i.e., to be valuable). Activities in this phase may refer to keeping information up to date and other kinds of information management activities (e.g., enhancing, cleansing, merging and removing duplicate information in data warehouses).

• **Dispose**—The phase in which the information resource is transferred or retained for a defined period, destroyed, or handled as part of an archive as needed. Activities in this phase may refer to information retention, archiving or destroying.

The IS auditor should ensure that the quality of the data allows the organization to meet its strategic objectives. Are the data being captured and processed to required standards? The IS auditor should also ensure that the configuration of the organization's applications and database management systems is in line with organizational objectives. For example, are data being

archived, retained or destroyed in line with a data retention policy?

4.7 SYSTEMS PERFORMANCE MANAGEMENT

Systems performance refers to the study of an entire system, including physical hardware and components and software, and how it operates.

Enterprises want to ensure that systems are performing as expected and issues are identified and addressed in a timely fashion. It is important to understand the features of the IS architecture and associated software to aid in the systems performance management process.

4.7.1 IS ARCHITECTURE AND SOFTWARE

The architecture of most computers can be viewed as a number of layers of circuitry and logic, arranged in a hierarchical structure that interacts with the computer's OS. At the base of the hierarchy is the computer hardware, which includes some hard-coded instructions (firmware). The next level up in the hierarchy comprises the nucleus (kernel) functions. Functions of the nucleus relate to basic processes associated with the OS, which include:

- Interrupt handling
- Process creation/destruction
- Process state switching
- Dispatching
- Process synchronization
- Interprocess communication
- Support of I/O processes

• Support of the allocation and reallocation/release of memory

The nucleus is a highly privileged area where access by most users is restricted. Above the nucleus are various OS processes that support users.

These processes, referred to as system software, are a collection of computer programs used in the design, processing and control of all computer applications used to operate and maintain the computer system. Comprised of system utilities and programs, the system software ensures the integrity of the system, controls the flow of programs and events in the computer, and manages the interfaces with the computer. Software developed for the computer must be compatible with its OS. Examples include:

• Access control software

• Data communications software

• Database management software

• Program library management systems

• Tape and disk management systems

• Network management software

• Job scheduling software

• Utility programs

Some or all of the above may be built into the OS.

4.7.2 OPERATING SYSTEMS

Before discussion of the various forms of system software, the most significant system software related to a computer—its OS—needs to be further addressed. The OS contains programs that interface between the user, processor and applications software. It is the control program that runs the computer and acts as a scheduler and traffic controller. It provides the primary means of managing the sharing and use of computer resources, such as processors, real memory (e.g., RAM), auxiliary memory (e.g., disk storage) and I/O devices.

Most modern OSs have also expanded the basic OS functionalities to include capabilities for a more efficient operation of system and applications software. For example, all modern OSs possess a virtual storage memory capability that allows programs to use and reference a range of addresses greater than the real memory. This technique of mapping parts of a large slower memory to a faster and smaller working memory is used between various levels of cached memory within modern systems.

OSs vary in the resources managed, comprehensiveness of management and techniques used to manage resources. The type of computer, its intended use, and normal, expected attached devices and networks influence the OS

requirements, characteristics and complexity. For example, a single-user microcomputer operating in stand-alone mode needs an OS capable of cataloging files and loading programs to be effective.

A mainframe computer handling large volumes of transactions for consolidation and distribution requires an OS capable of managing extensive resources and many concurrent operations, in terms of application input and output, with a very high degree of reliability. For example, the z/OS

operating system from IBM has been engineered specifically to complement this environment.

A server with multiple users interacting with data and programs, from database servers and middleware connections to legacy mainframe

applications, requires an OS that can accommodate multiprocessing, multitasking and multithreading. It must be able to share disk space (files) and CPU time among multiple users and system processes and manage connections to devices on the network. For example, the UNIX operating system is designed to specifically address this type of environment.

A microcomputer in a networked environment functioning as a server with specialized functions (e.g., applications, database management systems

[DBMSs] and directory/file storage) also can interact with data and programs of multiple users to provide services to client workstations throughout the network.

It is common for OSs to run on virtual servers. In a virtual environment,

software is used to partition one physical server into multiple independent virtual servers. Each of these environments can then run its own (and if required different) OS. To the operator, the OS behaves as if it were running on a physical server.

Software Control Features or Parameters

Various OS software products provide parameters and options for the tailoring of the system and activation of features such as activity logging.

Parameters are important in determining how a system runs because they allow a standard piece of software to be customized to diverse environments.

Software control parameters deal with:

• Data management

• Resource management

• Job management

• Priority setting

Parameter selections should be appropriate to the organization’s workload and control environment structure. The most effective means of determining how controls are functioning within an OS is to review the software control features and/or parameters.

Improper implementation and/or monitoring of OSs can result in undetected errors and corruption of the data being processed and lead to unauthorized access and inaccurate logging of system usage.

Software Integrity Issues

OS integrity is a very important requirement and ability of the OS and involves using specific hardware and software features to:

• Protect itself from deliberate and inadvertent modification

• Ensure that privileged programs cannot be interfered with by user programs

• Provide for effective process isolation to ensure that:

– Multiple processes running concurrently will not interfere by accident or by design with each other and are protected from writing into each other's memory (e.g., changing instructions, sharing resources, etc.)

– Enforcement of least privilege where processes have no more privilege than needed to perform functions and modules call on more privileged routines only if, and for as long as, needed.

To maintain system and data integrity, it is necessary to correctly and consistently define, enforce and monitor the operating environment and the granted permissions. IS management is responsible for the implementation of appropriate authorization techniques to prevent nonprivileged users from gaining the ability to execute privileged instructions and thus take control of the entire machine.

For example, IBM mainframe z/OS systems are customized at system generation (SYSGEN) time. When these systems are started (initial program load), important options and parameters are read from information kept in a key system directory (referred to as the SYS1.PARMLIB partitioned data

set). The directory specifies critical initialization parameters that are used to meet the data center's installation requirements (i.e., other system software activated for job scheduling, security, activity logging, etc.). These options, if uncontrolled, provide a nonprivileged user a way to gain access to the OS's supervisory state. The IS auditor should review system configuration directories/files in all OSs for control options used to protect the supervisory state.

Likewise, PC-based client-server Windows, UNIX and Linux OSs have special system configuration files and directories. The existence of program flaws or errors in configuring, controlling and updating the systems to the latest security patches makes them vulnerable to being compromised by perpetrators. Important Windows system options and parameters are set in special system configuration files, referred to as a registry. Therefore, the registry is an important aspect of IS auditing. Noting any changes that take place in the registry is crucial for maintaining the integrity, confidentiality and availability of the systems. In UNIX-based OSs, the same issues are present. Critical system configuration files

and directories related to the nucleus (kernel) operations, system start-up, network file sharing and other remote services should be appropriately secured and checked for correctness.

Activity Logging and Reporting Options

Computer processing activity can be logged for analysis of system functions.

Following are some of the areas that can be analyzed based on the activity log:

• OS logs to:

– Identify data file versions used for production processing

– Evaluate programs scheduled and run

– Discover utilities or service IDs usage

– Evaluate OS activities to ensure that the integrity of the OS has not been compromised due to improper changes to system parameters and

libraries

• Databases to:

– Evaluate the efficiency of the database structure

– Identify database errors/failures

– Assess database security

• Access control to:

– Evaluate the access controls over critical data files/bases and programs

– Evaluate security facilities that are active in communications systems, DBMSs and applications

Many intruders will attempt to alter logs to hide their activities. Secure logging is also needed to preserve evidence authenticity should the logs be required for legal/court use. It is, therefore, important that logs are protected against

alteration. A common way to achieve this is to capture, centralize and analyze the logs on a secure server using security information and event management (SIEM) software.

Operating System Reviews

When auditing operating software development, acquisition or maintenance, the details shown in **figure 4.5** should be considered.

4.7.3 ACCESS CONTROL SOFTWARE

Access control software is designed to prevent unauthorized access to data, unauthorized use of system functions and programs, and unauthorized updates/changes to data, and to detect or prevent unauthorized attempts to access computer resources. For more details on access control software, see

chapter 5, Protection of Information Assets.

Figure 4.5—Operating Systems Reviews

Areas to Review	Questions to Consider
• System software selection	• Do they align with the enterprise architecture?
procedures	• Do they comply with short- and long-range IS plans?
	• Do they meet the IS requirements?
	• Are they properly aligned with the objectives of the business?
	• Do they include IS processing and control requirements?
	• Do they include an overview of the capabilities of the software and control options?

• Feasibility study

• Are same selection criteria applied to all proposals?

• Selection process

• Has the cost-benefit analysis of system software procedures

addressed:

– Direct financial costs associated with the product?

– Cost of product maintenance?

– Hardware requirements and capacity of the product?

– Training and technical support requirements?

– Impact of the product on processing reliability?

– Impact on data security?

– Financial stability of the vendor’s operations?

• System software security

• Have procedures been established to restrict the ability to

circumvent logical security access controls?

• Have procedures been implemented to limit access to the system interrupt capability?

• Have procedures been implemented to manage software patches

and keep the system software up-to-date?

• Are existing physical and logical security provisions adequate to restrict access to the master consoles?

• Were vendor-supplied installation passwords for the system

software changed at the time of installation?

• IT asset management

• Has an owner been designated?

• Have we retained a copy of the contracts/SLAs?

• What is the license agreement? Are we in compliance with it?

• System software

• Are controls adequate in:

implementation

– Change procedures?

– Authorization procedures?

– Access security features?

– Documentation requirements?

– Documentation of system testing?

– Audit trails?

– Access controls over the software in production?

• Authorization

• Have additions, deletions or changes to access authorization been documentation

documented?

• Does documentation exist of any attempted violations? If so, has there been follow-up?

• System documentation

• Are the following areas adequately documented:

– Installation control statements?

– Parameter tables?

– Exit definitions?

– Activity logs/reports?

• System software

• Is documentation available for changes made to the system

maintenance activities

software?

• Are current versions of the software supported by the vendor?

• Is there a defined patching process?

• System software change

• Is access to the libraries containing the system software limited to controls

individual(s) needing to have such access?

• Are changes to the software adequately documented and tested

prior to implementation?

• Is software authorized properly prior to moving from the test

environment to the production environment?

• Controls over the

• Have all appropriate levels of software been implemented?

installation of changed

• Have predecessor updates taken place?

system software

• Are system software changes scheduled for times when the changes least impact IS processing?

• Has a written plan been established for testing changes to system software?

• Are test procedures adequate to provide reasonable assurance that changes applied to the system correct known problems and that

they do not create new problems?

• Are tests being completed as planned?

• Have problems encountered during testing been resolved and were the changes retested?

• Have fallback or restoration procedures been put in place in case of production failure?

4.7.4 DATA COMMUNICATIONS SOFTWARE

Data communications software is used to transmit messages or data from one point to another either locally or remotely. For example, a database request from an end user is transmitted from that user's terminal to an online application, then to a DBMS in the form of messages handled by data communications software. Likewise, responses back to the user are handled in the same manner (i.e., from the DBMS to the online application and back to the user's terminal).

A typical simple data communications system has three components: 1. The transmitter (source)

2. The transmission path (channel or line)

3. The receiver

One-way communication flows in one direction only. In a two-way

communication, both ends may simultaneously operate as source and receiver,

with data flowing over the same channel in both directions. The data communication system is concerned only with the correct transmission between two points. It does not operate on the content of the information.

A data communication system is divided into multiple functional layers. At each layer, software interfaces with hardware to provide a specific set of functions. All data communication systems have at least a physical layer and a data link layer. (See chapter 5, Protection of Information Assets, for more

information.)

Communication-based applications operate in local area network (LAN) and wide area network (WAN) environments to support:

• Electronic funds transfer (EFT) systems

• Database management systems

• Customer electronic services/electronic data interchange (EDI)

• Internet forums and email The data communication system interfaces with the OS, application programs, database systems, telecommunication address method systems, network control system, job scheduling system and operator consoles.

4.7.5 UTILITY PROGRAMS

Utility programs are system software used to perform maintenance and routines that frequently are required during normal processing operations.

Utility programs can be categorized by use, into five functional areas: 1. Understanding application systems (flowcharting software, transaction profile analyzer, executive path analyzer and data dictionary)

2. Assessing or testing data quality (data manipulation utilities, database dump utilities, data comparison utility and query facility)

3. Testing a program’s ability to function correctly and maintain data integrity (test data generator, online debugging facility, output analyzer and network simulator)

4. Assisting in faster program development (visual display utility, library copy, text editor, online coding facility, report generators and code generators)

5. Improving operational efficiency (CPU and memory utilization monitors and communication line analyzers)

Smaller computer systems (i.e., PC and server OSs) are often equipped with specific utilities to:

• Operate verification, cleaning and defragmenting of hard disk and removable memory units

• Initialize removable data volumes and volumes of disk/removable memory

• Save/restore system images

• Reconstruct and restore (logically) cancelled files

• Test system units and peripherals

Many of these utility programs can perform outside the security system or can function without producing an audit trail of activity. As a result, access to and use of these sensitive and powerful utilities should be well controlled and restricted.

4.7.6 SOFTWARE LICENSING ISSUES

Software copyright laws must be followed to protect against the possibility of a company paying penalties over copyright infringements and the added reputational risk of being identified as a company that illegally uses software.

A software licensing agreement is a contract that establishes the terms and conditions under which a piece of software is being licensed (i.e., made legally available for use) from the software developer (owner) to the user.

There are two different software licensing types: free (**figure 4.6**) and paid

(figure 4.7).

Figure 4.6—Free Software Licensing Types

Type

Description

Open source

The software may be used, copied, studied, modified and

redistributed as required. Open source is usually accompanied by the program source and a copy of the software license (for example, the GNU General Public License). A well-known example is Linux.

Freeware

The software is free, but the source code cannot be redistributed. A well-known example is Adobe Acrobat Reader®.

Shareware

The software may be free initially; however, this may only be on a trial basis or have limited functionality compared to the full,

commercial version (may also be known as trial version, demo ware or an evaluation copy).

Figure 4.7—Paid Software Licensing Types

Type

Description

Per central processing unit

Depends on the power of the server, specifically the number of the (CPU)

CPUs; could include the number of CPU cores

Per seat

Depends on the number of unique users of the system

Concurrent users

Depends on the total number of users using the software within a predefined period of time

Utilization

Depends on how busy the CPU is or the number of users that are

active at any one time

Per workstation

Depends on the number of individual workstations (NOT users) that connect to the software

Enterprise

Usually allows unlimited use of the software throughout an

organization without the need to apply any of the rules above,

although there may be some restrictions

To detect software licensing violations, the IS auditor should:

• Review the listing of all standard, used and licensed application and system software.

• Obtain copies of all software contracts for these to determine the nature of the license agreements, be it an unlimited enterprise license, per-seat license or individual copies.

• Scan the entire network to produce a list of installed software.

• If required, review a list of server specifications including CPUs and cores.

• Compare the license agreements with the software that is actually installed noting any violations.

Options available to prevent software license violations include:

• Ensure a good software asset management process exists (see section 4.2, IT Asset Management).

• Centralize control, distribution and installation of software (includes disabling the ability of users to install software, where possible).

• Require that all PCs be restricted workstations with disabled or locked-down disk drives, USB ports, etc.

• Install metering software on the LAN and require that all PCs access applications through the metered software.

• Regularly scan user networks endpoints to ensure that unauthorized copies of software have not been loaded (achieved by comparing actual software loaded to the list of software assets).

• Enforce documented policies and procedures that require users to sign an agreement not to install software without management authorization and a

software license agreement.

Software licenses are primarily contractual compliance—that is,

organizations agree to comply with the terms and conditions of the software publisher, with or without financial consideration. In certain circumstances, an IS auditor may need expert legal opinion to confirm compliance.

Note that some disaster recovery arrangements may require additional licenses and hosting of additional metering software. See section 4.16, Disaster Recovery Plans, for more information.

4.7.7 SOURCE CODE MANAGEMENT

Source code is the language in which a program is written. It is translated into object code by assemblers and compilers and tells the computer what to do.

By its very nature, source code may contain intellectual property and should be protected, and access should be restricted.

Organizational access to source code may differ depending on the application

and the nature of the agreement with the supplier. If no source code is supplied, it may be important to secure an escrow agreement. If the software is packaged, access to the source code may be granted under license to allow for customized modifications. If the software is bespoke or developed in house, the organization will have full access to the source code. In all instances source code is subject to the software development life cycle (see section 3.3, System Development Methodologies). Source code management is also tightly linked to change management, release management, quality assurance and information security management.

The actual source code should be managed using a version control system (VCS), often called revision control software (RCS). These maintain a central repository, which allows programmers to check out a program source to make changes to it. Checking in the source creates a new revision of the program. A VCS provides the ability to synchronize source changes with changes from other developers, including conflict resolution when changes have been made to the same section of source. A VCS also allows for branching, a copy of the trunk (original main code) that exists independently

to allow for customization for different customers, countries, locations etc.

An example of a popular VCS is Apache™ Subversion®. Git is a distributed version control system (DVCS). While Subversion manages a single centralized repository, a DVCS has multiple repositories. In a DVCS, the entire repository may be replicated locally with changes committed to the master repository when needed. This allows developers to work remotely, without a connection.

The advantages of VCSs include:

• Control of source code access

• Tracking of source code changes

• Allowing for concurrent development

• Allowing rollback to earlier versions

• Allowing for branching

The IS auditor should always be aware of the following:

• Who has access to source code

• Who can commit the code (push the code to production)

• Alignment of program source code to program objects

• Alignment with change and release management

• Backups of source code including those offsite and escrow agreements **4.7.8 CAPACITY MANAGEMENT**

Capacity management is the planning and monitoring of computing and network resources to ensure that the available resources are used efficiently and effectively. This requires that the expansion or reduction of resources takes place in parallel with the overall business growth or reduction. The capacity plan should be developed based on input from user and IS

management to ensure that business goals are achieved in the most efficient and effective way. This plan should be reviewed and updated at least annually.

Capacity planning should include projections substantiated by experience, considering the growth of existing business and future expansions. The following information is key to the successful completion of this task:

• CPU utilization

• Computer storage utilization

• Telecommunications

• LAN and WAN bandwidth utilization

• I/O channel utilization

• Number of users

• New technologies

• New applications

• Service level agreements (SLAs)

The IS auditor must realize that the amount and distribution of these requirements have intrinsic flexibility. Specialized resources of a given class may have an impact on the requirements for other classes. For example, the proper use of more intelligent terminals may consume less processor power and less communications bandwidth than other terminals. Consequently, the previous information is strictly related to type and quality of used or planned system components.

An element in capacity management is deciding whether to host the organization's applications distributed across several small servers, consolidated onto a few large servers, in the cloud or combinations of the three hosts. Consolidating applications on a few large servers (also known as application stacking) often allows the organization to make better overall use of the resources, but it increases the impact of a server outage, and it affects more applications when the server has to be shut down for maintenance.

Using the cloud allows extra capacity to be purchased on demand, but also brings the risk of relying on the supplier.

Larger organizations often have hundreds, if not thousands, of servers that are arrayed in groups referred to as server farms. Where virtual servers are used, these may be organized as private (also known as internal or corporate) clouds.

If an organization has put data storage hardware in place, the IS auditor should review the capacity management plans, which involve data storage utilization and storage area network (SAN) utilization.

Capacity management must also include network devices, such as switches and routers, that comprise physically and logically separated networks (virtual local area networks [VLANs]).

Capacity planning defines the business's requirements for IT capacity, in business and technical terms, and presents the consequences of delivering the required volume of activity through the IT infrastructure and applications—at the right time and with optimal cost. Capacity management ensures that all current and future capacity and performance aspects of the business requirements are provided in a cost-effective manner.

Information system capacity is one of the key business requirements for IT

systems. Business operations and processes can only be supported reliably when IT systems provide the required capacity. IT management should understand the capacity requirements prior to the design of their information systems and verify the final design against the capacity requirements. IT

management also must monitor capacity on an ongoing basis and provide additional capability as the business grows. For example, a file server may store all business files, but in two years, when the storage reaches the 80

percent threshold, an additional hard disk should be installed to keep up with the storage requirements.

IT capacity—as measured by CPU power and size of memory, hard disk or servers—is expensive. Organizations do not want to acquire more than what they need at the present time. Capacity planning is the process of ensuring that the resource provision can always meet business requirements. By continuously monitoring the threshold of the capacity utilization, additional capacity can be acquired and deployed before it no longer meets business requirements. With capacity management, expensive resources will only be provided when they are needed, thus resulting in a cost savings.

Capacity management monitors resource utilization and helps with resource planning. During procurement of the IT system, the capability management team will work with the architect to estimate resource requirements and to ensure that adequate, but not excessive, resources are provided to support the new solutions. The estimate is normally based on number of transactions, size

of data being stored, transaction processing time and response time, etc.

Estimates help determine capability requirements for the new solutions.

Capacity management aims to consistently provide the required IT resources

—at the right time and cost and in alignment with current and future requirements of the business. Capacity management increases efficiency and cost savings by deferring the cost of new capacity to a later date and optimizing capacity to business needs. Capacity management reduces the risk of performance problems or failure by monitoring the resource utilization threshold and provision of new resources before a shortage occurs. Capacity management also provides accurate capacity forecasting through application sizing and

modeling for new services.

Capacity planning and monitoring includes the elements listed in **figure 4.8**.

Figure 4.8—Capacity Planning and Monitoring Elements

Development

Develop a capacity plan that describes current and future

requirements for capacity of IT resources.

Monitoring

Monitor IT components to ensure that agreed-upon service levels are achieved.

Analysis

Analyze data collected from monitoring activities to identify trends from which normal utilization and service level, or baseline, can be established.

Tuning

Optimize systems for actual or expected workload based on analyzed and interpreted monitoring data.

Implementation

Introduce changes or new capacity to meet new capacity

requirements.

Modeling

Model and forecast the behavior of IT resources to determine future capacity trends and requirements.

Application sizing

Take into consideration the predicted resources for new capacity.

When designing the application, determine its size (number of

concurrent users that can be handled, number of transactions and data storage requirements) and required server capability, memory size, processing power, etc.

4.8 PROBLEM AND INCIDENT MANAGEMENT

Computer resources, like any other organizational asset, should be used in a manner that benefits the entire organization. This includes providing information to authorized personnel when and where it is needed, and at a cost that is identifiable and auditable. Computer resources include hardware, software, telecommunications, networks, applications and data.

Controls over these resources are sometimes referred to as general controls.

Effective control over computer resources is critical because of the reliance on computer processing in managing the business.

4.8.1 PROBLEM MANAGEMENT

Problem management aims to resolve issues through the investigation and in-depth analysis of a major incident or several incidents that are similar in nature to identify the root cause. Standard methodologies for root cause analysis include the development of fishbone/Ishikawa cause-and-effect diagrams, brainstorming and the use of the 5 Whys—an iterative question-asking technique used to explore the cause-and-effect relationships underlying a problem.

After a problem is identified and analysis has identified a root cause, the condition becomes a \known error. A workaround can then be developed to address the error state and prevent future occurrences of the related incidents.

This problem is then added to the known error database (KEDB). The goal is to proactively prevent reoccurrence of the error elsewhere or, at a minimum, have a workaround that can be provided immediately should the incident reoccur.

Problem management and incident management are related but have different methods and objectives. Problem management’s objective is to reduce the number and/or severity of incidents, while incident management’s objective is to return the affected business process back to its normal state as quickly as

possible, minimizing the impact on the business. Effective problem management can show a significant improvement in the quality of service of an IS organization.

4.8.2 PROCESS OF INCIDENT HANDLING

Incident management is one of the critical processes in IT service management (ITSM). See section 4.10, IT Service Level Management, for more information. IT needs to be attended to on a continuous basis to better serve the customer. Incident management focuses on providing increased continuity of service by reducing or removing the adverse effect of disturbances to IT services and covers almost all nonstandard operations of IT services—thereby defining the scope to include any nonstandard event. In addition to initiation, other steps in the incident life cycle include classification, assignment to specialists, resolution and closure.

It is essential for any incident handling process to prioritize items after determining the impact and urgency. For example, there could be a situation where a service request from the chief information officer (CIO) for a printer problem arrives at the same time as a request from the technology team to attend to a server crash. IS management should have parameters in place for assigning the priority of these incidents, considering both the urgency and impact.

Unresolved incidents are escalated based on the criteria set by IS

management. Incident management is reactive, and its objective is to respond to and resolve issues restoring normal service (as defined by the SLA) as quickly as possible. Formal SLAs are sometimes in place to define acceptable ranges for various incident management statistics.

4.8.3 DETECTION, DOCUMENTATION, CONTROL,

RESOLUTION AND REPORTING OF ABNORMAL

CONDITIONS

Because of the highly complex nature of software, hardware and their interrelationships, a mechanism should exist to detect and document any abnormal conditions that could lead to the identification of an error. This documentation generally takes the form of an automated or manual log. See

figures 4.9 and 4.10.

Figure 4.9—Typical Types of Errors That Are Logged

• Application errors

• Network errors

• System errors

• Telecommunication errors

• Operator errors

• Hardware errors

Figure 4.10—Items to Appear in an Error Log Entry

• Error date

• Initials of the individual responsible for closing the log entry

• Error resolution

• Department/center responsible for error resolution

description

• Status code of problem resolution (i.e., problem open, problem

• Error code

closed pending some future specified date, or problem irresolvable

• Error description

in current environment)

• Source of error

• Narrative of the error resolution status

• Escalation date and time

• Initials of the individual

responsible for

maintaining the log

For control purposes, the ability to add to the error log should not be restricted. The ability to update the error log, however, should be restricted to authorized individuals, and the updates should be traceable. Proper segregation of duties requires that the ability to close an error log entry be assigned to a different individual than the one responsible for maintaining or initiating the error log entry.

IS management should ensure that the incident and problem management mechanisms are properly maintained and monitored and that outstanding errors are being adequately addressed and resolved in a timely manner.

IS management should develop operations documentation to ensure that procedures exist for the escalation of unresolved problems to a higher level of IS management. While there are many reasons why a problem may remain outstanding for a long period of time, it should not be acceptable for a problem to remain unresolved indefinitely. The primary risk resulting from lack of attention to unresolved problems is the interruption of business operations. An unresolved hardware or software problem could potentially corrupt production data. Problem escalation procedures should be well documented. IS management should ensure that the problem escalation procedures are being adhered to properly. Problem escalation procedures

generally include:

• Names/contact details of individuals who can deal with specific types of problems

• Types of problems that require urgent resolution

• Problems that can wait until normal working hours

Problem resolution should be communicated to appropriate systems,

programming, operations and user personnel to ensure that problems are resolved in a timely manner. The IS auditor should examine problem reports and logs to ensure that they are resolved in a timely manner and are assigned to the individuals or groups most capable of resolving the problem.

The departments and positions responsible for problem resolution should be part of problem management documentation. This documentation must be maintained properly to be useful.

4.8.4 SUPPORT/HELP DESK

The responsibility of the technical support function is to provide specialist knowledge of production systems to identify and assist in system change/development and problem resolution. In addition, it is technical support's responsibility to apprise management of current technologies that may benefit overall operations.

Procedures covering the tasks to be performed by the technical support personnel must be established in accordance with an organization's overall strategies and policies. **Figure 4.11** illustrates common support functions.

Figure 4.11—Typical Support Functions

• Determine the source of computer incidents and take appropriate corrective actions.

• Initiate problem reports, as required, and ensure that incidents are resolved in a timely manner.

• Obtain detailed knowledge of the network, system and applications.

• Answer inquiries regarding specific systems.

• Provide second- and third-tier support to business user and customer.

• Provide technical support for computerized telecommunications processing.

• Maintain documentation of vendor software, including issuance of new releases and problem fixes, as well as documentation of utilities and systems developed in house.

• Communicate with IS operations to signal abnormal patterns in calls or application behavior.

Support is generally triaged when a help desk ticket/call is initiated and then escalated based on the complexity of the issue and the level of expertise required to resolve the problem.

The primary purpose of the help desk is to service the user. The help desk personnel must ensure that all hardware and software incidents that arise are fully documented and escalated based on the priorities established by management. In many organizations, the help desk function means different things. However, the basic function of the help desk is to be the first, single and central point of contact for users and to follow the incident management process.

4.8.5 NETWORK MANAGEMENT TOOLS

In an organization's modern inter-networking environment, all the tasks in

figure 4.11 can be accomplished by a set of tools generically called network management tools.

Response time reports identify the time necessary for a command entered by a user at a terminal to be answered by the host system. Response time is important because end users experiencing slow response time will be reluctant to utilize IS resources to their fullest extent. These reports typically identify average, worst and best response times over a given time interval for individual telecommunication lines or systems. These reports should be reviewed by IS management and system support personnel to track potential problems. If response time is slow, all possible causes, such as I/O channel bottlenecks, bandwidth utilization and CPU capacity, should be investigated; various solutions should be analyzed; and an appropriate and cost-justified corrective action should be taken.

Downtime reports track the availability of telecommunication lines and circuits. Interruptions due to power/line failure, traffic overload, operator error or other anomalous conditions are identified in a downtime report. If downtime is excessive, IS management should consider the following remedies:

• Add or replace telecommunications lines.

• Switch to a more dependable transmission link (such as dedicated lines

versus shared lines).

• Install backup power supplies.

• Improve access controls.

• Closely monitor line utilization to better forecast user needs, both in the near and long term.

Help desk reports are prepared by the help desk, which is staffed or supported by IT technicians who are trained to handle problems occurring during normal IS usage. If an end user encounters any problem, he/she can contact the help desk for assistance. Help desk facilities are critical to the telecommunication environment since they provide end users with an easy means of identifying and resolving problems quickly, before they have a major impact on IS performance and end-user resource utilization. Reports prepared by the help desk provide a history of the problems and their resolution.

Online monitors check data transmission accuracy and errors. Monitoring can be performed by echo checking (received data are bounced back to sender for verification) and status checking all transmissions, ensuring that messages are not lost or transmitted more than once.

Network monitors provide a real time display of network nodes and status.

Network (protocol) analyzers are diagnostic tools attached to a network link that use network protocols' intelligence for monitoring the packets flowing along the link and produce network usage reports. Network analyzers are typically hardware-based and operate at the data link and/or network level.

Output includes the following information:

• Protocol(s) in use

• Type of packets flowing along the monitored link

• Traffic volume analysis

• Hardware errors, noise and software problems

• Other performance statistics (e.g., percentage of used bandwidth)

• Problems and possible solutions

Simple Network Management Protocol (SNMP) is a TCP/IP-based protocol that monitors and controls variables throughout the network, manages configurations and collects statistics on performance and security. A master console polls all the network devices on a regular basis and displays the global status. SNMP software is capable of accepting, in real-time, specific operator requests. Based on the operator instructions, SNMP software sends specific commands to an SNMP-enabled device and retrieves the required information. To perform all of these tasks, each device (e.g., routers, switches, hubs, PCs and servers) needs to have an SNMP agent running. The SNMP communication occur between all the agents and the console.

4.8.6 PROBLEM MANAGEMENT REPORTING REVIEWS

The audit approach shown in **figure 4.12** should be considered when reviewing problem management reporting.

Figure 4.12—Problem Management Reporting Reviews

Areas to Review	**Questions to Consider**
• Interviews with IS	

• Have documented procedures been developed to guide IS operations personnel

operations personnel in logging, analyzing, resolving and escalating problems in a timely manner, in accordance with management's intent and authorization?

• Procedures used by the IT

• Are procedures for recording, evaluating, and resolving or department

escalating any operating or processing problems ad equate?

• Operations documentation

• Are procedures used by the IT department to collect statistics regarding online processing performance adequate and is the analysis accurate and complete?

• Are all problems identified by IS operations being recorded for verification and resolution?

• Performance records •

• Do problems exist during processing?

Outstanding error log

• Are the reasons for delays in application program processing valid?

entries

• Are significant and recurring problems identified, and actions taken

• Help desk call logs

to prevent their recurrence?

• Were processing problems resolved in a timely manner and was the

resolution complete and reasonable?

• Are there any reoccurring problems that are not being reported to

IS management?

4.9 CHANGE, CONFIGURATION, RELEASE AND PATCH MANAGEMENT

Change control procedures are a part of the more encompassing function referred to as change management and are established by IS management to control the movement of application changes (programs, jobs, configurations, parameters, etc.) from the test environment, where development and maintenance occur, to the quality assurance (QA) environment, where thorough testing occurs, to the production environment. Typically, IS

operations are responsible for ensuring the integrity of the production environment and often serve as the final approvers of any changes to production.

Change management is used when changing hardware, installing or

upgrading to new releases of off-the-shelf applications, installing a software patch and configuring various network devices (e.g., firewalls, routers and switches).

The procedures associated with this process ensure that:

• All relevant personnel are informed of the change and when it is happening.

• System, operations and program documentation are complete, up to date and in compliance with the established standards.

• Job preparation, scheduling and operating instructions have been established.

• System and program test results have been reviewed and approved by user and project management.

• Data file conversion, if necessary, has occurred accurately and completely as evidenced by review and approval by user management.

• System conversion has occurred accurately and completely as evidenced by review and approval by user management.

• All aspects of jobs turned over have been tested, reviewed and approved by control/operations personnel.

• Legal or compliance aspects have been considered.

• The risk of adversely affecting the business operation are reviewed and a rollback plan is developed to back out the changes, if necessary.

Apart from change control, standardized methods and procedures for change management are needed to ensure and maintain agreed-on levels in quality service. These methods are aimed at minimizing the adverse impact of any probable incidents triggered by change that may arise.

This is achieved by formalizing and documenting the process of change request, authorization, testing, implementation and communication to the users. Change requests are often categorized into emergency changes, major changes and minor changes, and may have different change management procedures in place for each type of change.

4.9.1 PATCH MANAGEMENT

Patch management is an area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system to maintain up-to-date software and often to address security risk. Patch management tasks include the following:

• Maintain current knowledge of available patches.

• Decide what patches are appropriate for particular systems.

• Ensure that patches are installed properly; testing systems after installation.

• Document all associated procedures, such as specific configurations required.

Several products are available to automate patch management tasks. Patches can be ineffective and can cause more problems than they fix. To avoid problems, patch management experts suggest that system administrators take simple steps, such as performing backups and testing patches on non-critical systems prior to installations. Patch management can be viewed as part of change management.

See chapter 3, Information Systems Acquisition, Development and Implementation, for details on program change controls.

4.9.2 RELEASE MANAGEMENT

Software release management is the process through which software is made available to users. The term release is used to describe a collection of authorized changes. The release will typically consist of several problem

fixes and enhancements to the service.

The releases, whether major or minor, will have a unique identity.

Sometimes, the minor or small fixes may trigger some other problem. Fully tested, major releases may not have such problems. Because of testing time, space and other constraints, it is also possible to have a partial release, which is known as a delta release. The delta release contains only those items that have undergone changes since the last release.

The releases are controlled, and, if any problems arise in the new release, one should be able to back out completely and restore the system to its previous state. Suitable contingency plans may also be developed, if it is not completely restorable. These plans are developed before the new release is implemented. **Figure 4.13** shows some of the principal types of releases.

Many new system implementations will involve phased delivery of

functionality and thus require multiple releases. In addition, planned releases will offer an ongoing process for system enhancement.

The main roles and responsibilities in release management should be defined to ensure that everyone understands their role and level of authority and those of

others involved in the process. The organization should decide the most appropriate approach, depending on the size and nature of the systems, the number and frequency of releases required, and any special needs of the users (for example, if a phased rollout is required over an extended period of time).

All releases should have a unique identifier that can be used by configuration management.

Planning a release involves:

• Gain consensus on the release's contents.

• Agree to the release strategy (e.g., the phasing over time and by geographical location, business unit and customers).

• Produce a high-level release schedule.

Figure 4.13—Types of Releases

Major releases

Normally contain a significant change or addition of new

functionality. A major upgrade or release usually supersedes all preceding minor upgrades. Grouping together several changes

facilitates more comprehensive testing and planned user training.

Large organizations typically have a predefined timetable for

implementing major releases throughout the year (e.g., quarterly).

Smaller organizations may have only one release during the year or numerous releases if the organization is quickly growing.

Minor software releases

Upgrades, normally containing small enhancements and fixes. A

minor upgrade or release usually supersedes all preceding emergency fixes. Minor releases are generally used to fix small reliability or functionality

problems that cannot wait until the next major release.

The entire release process should be followed for the preparation and implementation of minor releases, but it is likely to take less time because the development, testing and implementation activities do not require as much time as major releases do.

Emergency software

Emergency releases are fixes that require implementation as quickly releases

as possible to prevent significant user downtime to business-critical functions. Depending upon the required urgency of the release,

limited testing and release management activities are executed prior to implementation. Such changes should be avoided whenever

possible because they increase the risk of errors being introduced.

• Plan resource levels (including staff overtime).

• Agree on roles and responsibilities.

• Produce back-out plans.

• Develop a quality plan for the release.

• Plan acceptance of support groups and the customer.

While change management is the process whereby all changes go through a robust testing and approval process, release management is the process of putting the software changes into production.

4.9.3 IS OPERATIONS

IS operations are processes and activities that support and manage the entire IS infrastructure, systems, applications and data, focusing on day-to-day activities.

IS operations staff is responsible for the accurate and efficient operation of the network, systems and applications and for the delivery of high-quality IS

services to business users and customers.

Tasks of the IS operations staff include:

• Execute and monitor scheduled jobs.

• Facilitate timely backup.

• Monitor unauthorized access and use of sensitive data.

• Monitor and review the extent of adherence to IS operations procedures as established by IS and business management.

• Participate in tests of disaster recovery plans (DRPs).

• Monitor the performance, capacity, availability and failure of information resources.

• Facilitate troubleshooting and incident handling.

Procedures detailing instructions for operational tasks and procedures coupled with appropriate IS management oversight are necessary parts of the IS control environment.

This documentation should include:

• Operations procedures that are based on operating instructions and job flows for computer and peripheral equipment

• Procedures for monitoring systems and applications

• Procedures for detecting systems and applications errors and problems

• Procedures for handling IS problems and escalation of unresolved issues

• Procedures for backup and recovery

IS Operations Reviews

Because processing environments vary among installations, a tour of the information processing facility generally provides the IS auditor with a better

understanding of operations tasks, procedures and control environment.

Audit procedures should include those shown in **figure 4.14.**

Figure 4.14—IS Operations Reviews

Areas to Review	Questions to Consider
• Observation of IS	• Have controls been put in place to ensure efficiency of operations personnel and adherence to established standards and policies? • Is adequate supervision present?
• Have controls been put in place regarding IS management review, data integrity and security?	
• Operator access	• Is access to files and documentation libraries restricted to operators? • Are responsibilities for the operation of computer and related peripheral equipment limited? • Is access to correcting program and data problems restricted? • Should access to utilities that allow system fixes to software and/or data be restricted? • Is access to production source code and data libraries (including run procedures) limited?
• Operator manuals	

• Are instructions adequate to address:

– The operation of the computer and its peripheral equipment?

– Startup and shutdown procedures?

– Actions to be taken in the event of machine/program failure?

– Records to be retained?

– Routine job duties and restricted activities?

• Access to the library

• Is the librarian prevented from accessing computer hardware?

• Does the librarian have access only to the tape management

system?

• Is access to library facilities provided to authorized staff only?

• Is removal of files restricted by production scheduling software?

• Does the librarian handle the receipt and return of foreign media entering the library?

• Are logs of the sign-in and sign-out of data files and media

maintained?

• Contents and location of

• Are offline file storage media containing production system

offline storage

programs and data clearly marked with their contents?

• Are offline library facilities located away from the computer room?

• Are policies and procedures adequate for:

– Administering the offline library?

– Checking out/in media, including requirements for signature

authorizations?

– Identifying, labeling, delivering and retrieving offsite backup files?

– Encryption of offsite backup files (especially if these physically move between locations)?

– Inventorying the system for onsite and offsite media, including the specific storage locations of each tape?

– Secure disposal/destruction of media, including requirements for signature authorizations?

• File handling procedures

• Have procedures been established to control the receipt and release of files and secondary storage media to/from other locations?

• Are internal tape labels used to help ensure that the correct media are mounted for processing?

• Are these procedures adequate and in accordance with

management’s intent and authorization?

• Are these procedures being followed?

• Data entry

• Are input documents authorized and do the documents contain

appropriate signatures?

• Are batch totals reconciled?

• Does segregation of duties exist between the person who keys the data and the person who reviews the keyed data for accuracy and

errors?

• Are control reports being produced? Are the reports accurate? Are the reports maintained and reviewed?

• Lights-out operations

• Remote access to the master console is often granted to standby operators for contingency purposes such as automated software

failure. Is access to security sufficient to guard against

unauthorized use?

• Do contingency plans allow for the proper identification of a

disaster in the unattended facility?

• Are the automated operation software and manual contingency

procedures documented and tested adequately at the recovery site?

• Are proper program change controls and access controls present?

• Are tests of the software performed on a periodic basis, especially after changes or updates are applied?

• Do assurances exist that errors are not hidden by the software and that all errors result in operator notification?

4.10 IT SERVICE LEVEL MANAGEMENT

The fundamental premise associated with ITSM is that IT can be managed through a series of discrete processes that provide service to the business.

Although each process area may have separate and distinct characteristics, each process is also highly interdependent with other processes. The processes, after defined, can be better managed through SLAs that serve to maintain and

improve customer satisfaction (i.e., with the end business).

ITSM focuses on the business deliverables and covers infrastructure management of IT applications that support and deliver these IT services.

This management includes fine tuning IT services to meet the changing demands of the enterprise and measuring and demonstrating improvements in the quality of IT services offered with a reduction in the cost of service in the long term.

IT services can be better managed with an SLA, and the services offered form a basis for such agreements. There is a possibility of a gap between customer

expectations and the services offered, and this is narrowed by the SLA, which completely defines the nature, type, time and other relevant information for the services being offered. SLAs can also be supported by operational level agreements (OLAs), which are internal agreements covering the delivery of services that support the IT organization in its delivery of services.

For example, when a complaint is received, the help desk looks for an available solution from the KEDB after classifying and storing the complaint as an incident. Repeated incidents or major incidents may lead to problems that call for the problem management process. If changes are needed, the change management group of the process/program can provide a supporting role after consulting the configuration management group.

Any required change—whether it originated as a solution to a problem, an enhancement or for any other reason—goes through the change management process. The cost-benefit and feasibility studies are reviewed before the changes are accepted and approved. The risk of the changes should be studied, and a fallback plan should be developed. The change may be for one configuration item or for multiple items, and the change management process invokes the configuration management process.

For example, the software can comprise different systems, each containing different programs and each program having different modules. The configuration can be maintained at the system level, the program level or the module level. The organization may have a policy saying that any changes made at the system level will be released as a new version. It may also decide to release a new version, if it involves changes at the program level for yet another application.

Service management metrics should be captured and appropriately analyzed so that this information can be used to enhance the quality of service. Many organizations have leveraged ITIL and/or ISO 20000 to improve their ITSM.

4.10.1 SERVICE LEVEL AGREEMENTS

An SLA is an agreement between the IT organization and the customer. The SLA details the service(s) to be provided. The IT organization could be an

internal IT department or an external IT service provider, and the customer is the business. The business may acquire IT services from an internal IT

organization, such as email services, an intranet, an enterprise resource planning (ERP) system, etc. The business may acquire IT services from an external IT service provider, such as Internet connectivity, hosting of the public website, etc.

The SLA describes the services in nontechnical terms, from the viewpoint of the customer. During the term of the agreement, it serves as the standard for measuring and adjusting the services.

Service-level management is the process of defining, agreeing on, documenting and managing levels of service that are required and cost justified. Service-level management deals with more than the SLAs themselves; it includes the production and maintenance of the service catalog, service review meetings and service improvement plans (SIPs) for areas that are not achieving their SLAs.

The aim of service-level management is to maintain and improve customer satisfaction and to improve the service delivered to the customer. With clear definition of service level, the IT organization or service provider can design the service based on the service level, and the customer can monitor the performance of the IT services. If the services provided do not meet the SLA, the IT organization or service provider must improve the services.

Characteristics of IT services are used to define the SLA. Characteristics that should be considered in the delivery of these services include accuracy, completeness, timeliness and security. Many tools are available to monitor the efficiency and effectiveness of services provided by IT personnel. These tools include:

• **Exception reports**—These automated reports identify all applications that did

not successfully complete or otherwise malfunctioned. An excessive number of exceptions may indicate:

– Poor understanding of business requirements

– Poor application design, development or testing

– Inadequate operation instructions

– Inadequate operations support

– Inadequate operator training or performance monitoring

– Inadequate sequencing of tasks

– Inadequate system configuration

– Inadequate capacity management

• **System and application log**s—Logs generated from various systems and applications should be reviewed to identify all application problems. These logs provide additional, useful information regarding activities performed on the computer because most abnormal system and application events will generate a record in the logs. Because of the size and complexity of the logs, it is difficult to manually review them. Programs have been developed that analyze the system log and report on specifically defined items. Using this software, the auditor can carry out tests to ensure that:

– Only approved programs access sensitive data.

– Only authorized IT personnel access sensitive data.

– Software utilities that can alter data files and program libraries are used only for authorized purposes.

– Approved programs are run only when scheduled and, conversely, unauthorized runs do not take place.

– The correct data file generation is accessed for production purposes.

– Data files are adequately protected.

• **Operator problem reports**—These manual reports are used by operators to log computer operations problems and their resolutions. Operator responses should be reviewed by IS management to determine whether operator actions were appropriate or whether additional training should be provided to operators.

• **Operator work schedules**—These schedules are generally maintained manually by IS management to assist in human resource planning. By ensuring proper staffing of operation support personnel, IS management is assured that service requirements of end users will be met. This is especially important during critical or heavy computer usage periods.

These schedules should be flexible enough to allow for proper cross-training and emergency staffing requirements.

Many IT departments define the level of service that they will guarantee to users of the IT services. This level of service is often documented in SLAs. It

is particularly important to define service levels where there is a contractual relationship between the IT department and the end user or customer. SLAs are often tied to chargeback systems, in which a certain percentage of the cost is apportioned from the end-user department to the IT department. When functions of the IT department are performed by a third party, it is important to have an outsourcing SLA.

Service levels are often defined to include hardware and software performance targets (such as user response time and hardware availability) but can also include a wide range of other performance measures. Such measures might include financial performance measures (e.g., year-to-year incremental cost reduction), human resources measures (e.g., resource planning, staff turnover, development or training) or risk management measures (e.g., compliance with control objectives). The IS auditor should be aware of the different types of measures available and should ensure that they are comprehensive and include risk, security and control measures as well as efficiency and effectiveness measures.

4.10.2 MONITORING OF SERVICE LEVELS

Defined service levels must be regularly monitored by an appropriate level of management to ensure that the objectives of IS operations are achieved. It is also important to review the impact on the customers and other stakeholders of the

organization.

For example, a bank may be monitoring the performance and availability of its automated teller machines (ATMs). One of the metrics may be availability of ATM services at expected levels (99.9 percent); however, it may also be appropriate to monitor the impact on customer satisfaction due to nonavailability. Similar metrics may be defined for other services, such as email and Internet.

Monitoring of service levels is essential for outsourced services, particularly if the third party is involved in directly providing services to an organization's customers. Failure to achieve service levels will have more of an impact on the organization than on the third party. For example, a fraud due to control weakness at a third party may result in reputation loss for the

organization.

It is important to note that when service delivery is outsourced, only responsibility for serviced provision is outsourced—accountability is not and still rests with the organization. If the organization outsources service delivery, the IS auditor should determine how management gains assurance that the controls at the third party are properly designed and operating effectively. Several techniques can be used by management, including questionnaires, onsite visits or an independent third-party assurance report, such as a Statement on Standards for Attestation Engagements 18 (SSAE 18) Service Organization Control (SOC) 1 report or AT-101 (SOC 2 and SOC 3) report.

4.10.3 SERVICE LEVELS AND ENTERPRISE ARCHITECTURE

Defining and implementing an enterprise architecture (EA) helps an organization in aligning service delivery (see section 2.5, Enterprise Architecture, for more information). Organizations may use multiple service delivery channels, such as mobile apps, the Internet, service outlets, third-party service providers and automated kiosks. These channels use different technologies that are serviced by the same backend database.

When considering availability and recovery options, EA best helps in aligning operational requirements that can address the service delivery objectives. For

example, an unacceptable recovery time may lead in choosing fault-tolerant, high-availability architecture for critical service delivery channels (see section 4.16.3, Recovery Alternatives, for more information).

4.11 DATABASE MANAGEMENT

DBMS software aids in organizing, controlling and using the data needed by application programs. A DBMS provides the facility to create and maintain a well-organized database. Primary functions include reduced data redundancy, decreased access time and basic security over sensitive data.

DBMS data are organized in multilevel schemes, with basic data elements,

such as the fields (e.g., Social Security number) at the lowest level. The levels above each field have differing properties depending on the architecture of the database.

The DBMS can include a data dictionary that identifies the fields, their characteristics and their use. Active data dictionaries require entries for all data elements and assist application processing of data elements, such as providing validation characteristics or print formats. Passive dictionaries are only a repository of information that can be viewed or printed.

A DBMS can control user access at the following levels:

• User and the database

• Program and the database

• Transaction and the database

• Program and data field

• User and transaction

• User and data field

Some of the advantages of a DBMS include:

• Data independence for application systems

• Ease of support and flexibility in meeting changing data requirements

• Transaction processing efficiency

• Reduction of data redundancy

• Ability to maximize data consistency

• Ability to minimize maintenance cost through data sharing

• Opportunity to enforce data/programming standards

• Opportunity to enforce data security

• Availability of stored data integrity checks

• Facilitation of terminal users' ad hoc access to data, especially through designed query language/application generators

4.11.1 DBMS ARCHITECTURE

Data elements required to define a database are called metadata. This includes data about data elements used to define logical and physical fields, files, data relationships, queries, etc. There are three types of metadata: conceptual schema, external schema and internal schema. If the schemas are

not adjusted to smoothly work together, the DBMS may not be adequate to meet the users' needs.

Detailed DBMS Metadata Architecture

Within each level, there is a data definition language (DDL) component for creating the schema representation necessary for interpreting and responding to the user's request. At the external level, a DBMS will typically accommodate multiple DDLs for several application programming languages compatible with the DBMS. The conceptual level will provide appropriate mappings between the external and internal schemas. External schemas are location independent of the internal schema.

Data Dictionary/Directory System

A data dictionary/directory system (DD/DS) helps define and store source and object forms of all data definitions for external schemas, conceptual schemas, the internal schema and all associated mappings. The data dictionary contains an index and description of all the items stored in the database. The directory describes the location of the data and the access method.

DD/DS provides the following functional capabilities:

• A data definition language processor, which allows the database administrator to create or modify a data definition for mappings between external and conceptual schemas

• Validation of the definition provided to ensure the integrity of the metadata

• Prevention of unauthorized access to, or manipulation of, the metadata

• Interrogation and reporting facilities that allow the DBA to make inquiries on the data definition

DD/DS can be used by several DBMSs; therefore, using one DD/DS could reduce the impact of changing from one DBMS to another DBMS. Some of the benefits of using DD/DS include:

• Enhance documentation.

• Provide common validation criteria.

• Facilitate programming by reducing the needs for data definition.

• Standardize programming methods.

4.11.2 DATABASE STRUCTURE

There are three major types of database structure: hierarchical, network and relational. Most DBMSs have internal security features that interface with the OS access control mechanism/package. A combination of the DBMS security features and security package functions is often used to cover all required security functions. Types of DBMS structures are discussed in the following paragraphs.

Hierarchical database model—In this model there is a hierarchy of parent and child data segments. To create links between them, this model uses parent-child relationships. These are 1:N (one-to-many) mappings between record types represented by logical trees, as shown in **figure 4.15**. A child segment is restricted to having only one parent segment, so data duplication is necessary to express relationships to multiple parents. Subordinate segments are retrieved through the parent segment. Reverse pointers are not allowed. When the data relationships are hierarchical, the database is easy to implement, modify and search. The registry in Microsoft Windows is an example of a hierarchical database. They are also used in geographic information systems.

Network database model—In the network model, the basic data modeling construct is called a set. A set is formed by an owner record type, a member record type and a name. A member record type can have that role in more than one set, so a multiowner relationship is allowed. An owner record type can also be a member or owner in another set. Usually, a set defines a 1:N

relationship, although one-to-one (1:1) is permitted. A disadvantage of the network model is that such structures can be extremely complex and difficult to comprehend, modify or reconstruct in case of failure. This model is rarely used in current environments. See **figure 4.16**. The hierarchical and network models do not support high-level queries. The user programs must navigate the data structures.

Relational database model—An example of a relational database can be seen in **figure 4.17**. The relational model is based on the set theory and relational calculations. A relational database allows the definition of data structures, storage/retrieval operations and integrity constraints. In such a

Figure 4.15—Organization of a Hierarchical Database

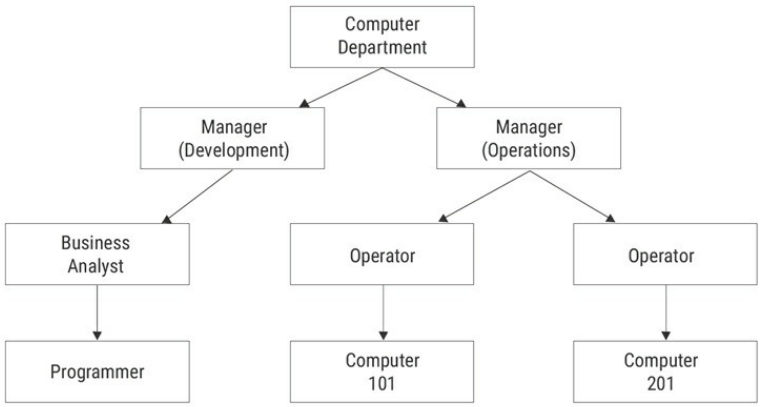
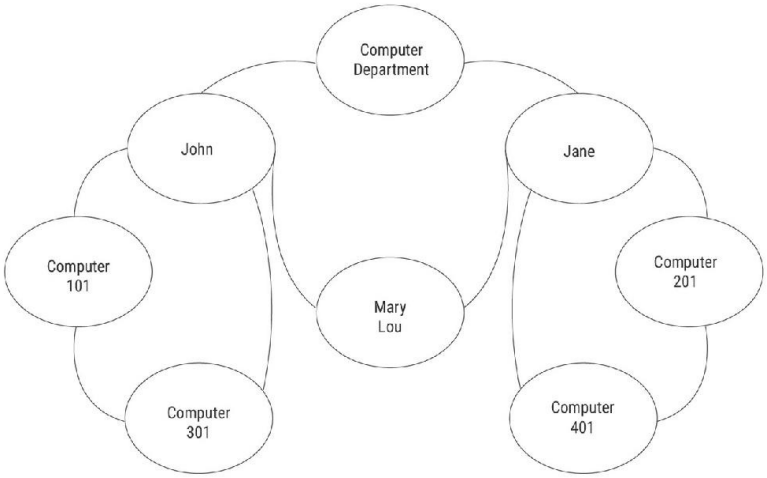


Figure 4.16– Organization of a Network Database



database, the data and relationships among these data are organized in tables.

A table is a collection of rows, also known as tuples, and each tuple in a table contains the same columns. Columns, called domains or attributes, correspond to fields. Tuples are equal to records in a conventional file structure. Relational databases are used in most common ERP Systems.

Common relational database management systems (RDBMS) include

Oracle®, IBM® DB2® and Microsoft SQL Server.

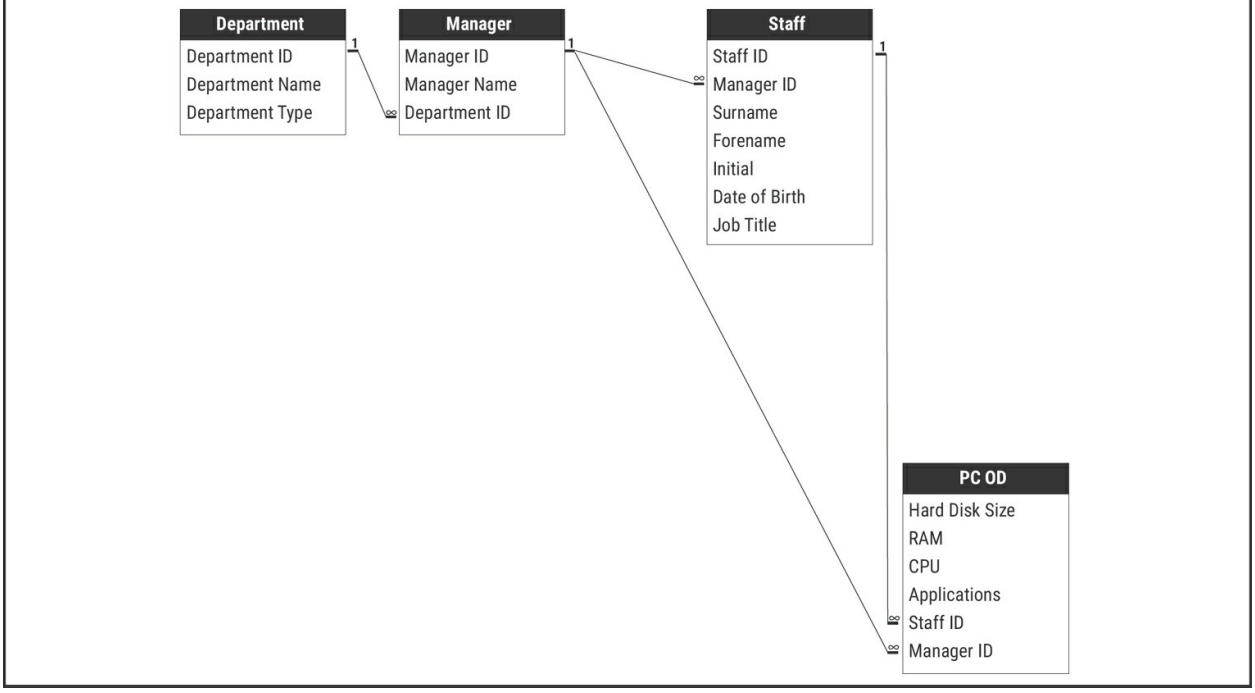
Relational tables have the following properties:

• Values are atomic, i.e., a single unit that is irreducible

• Each row is uniquely identifiable.

• Column values are of the same kind.

Figure 4.17—Organization of a Relational Database



• The sequence of columns is insignificant.

• The sequence of rows is insignificant.

• Each column has a unique name.

Certain fields may be designated as keys, so searches for specific values of that field will be quicker because of the use of indexing. If fields in two different tables take their values from the same set, a join operation can be performed to select related records in the two tables by matching values in those fields. This can be extended to joining multiple tables on multiple fields. These relationships are only specified at retrieval time, so relational databases are dynamic. The relational model is independent from the physical implementation of the data structure and has many advantages over the hierarchical and network database models. With relational databases, it is easier:

• For users to understand and implement a physical database system

• To convert from other database structures

• To implement projection and join operations (i.e., reference groups of related data elements not stored together)

• To create new relations for applications

• To implement access control over sensitive data

• To modify the database

A key feature of relational databases is the use of normalization rules to minimize the amount of information needed in tables to satisfy the users'

structured and unstructured queries to the database. Generally followed, normalization rules include:

• A given instance of a data object has only one value for each attribute.

• Attributes represent elementary data items; they should contain no internal structure.

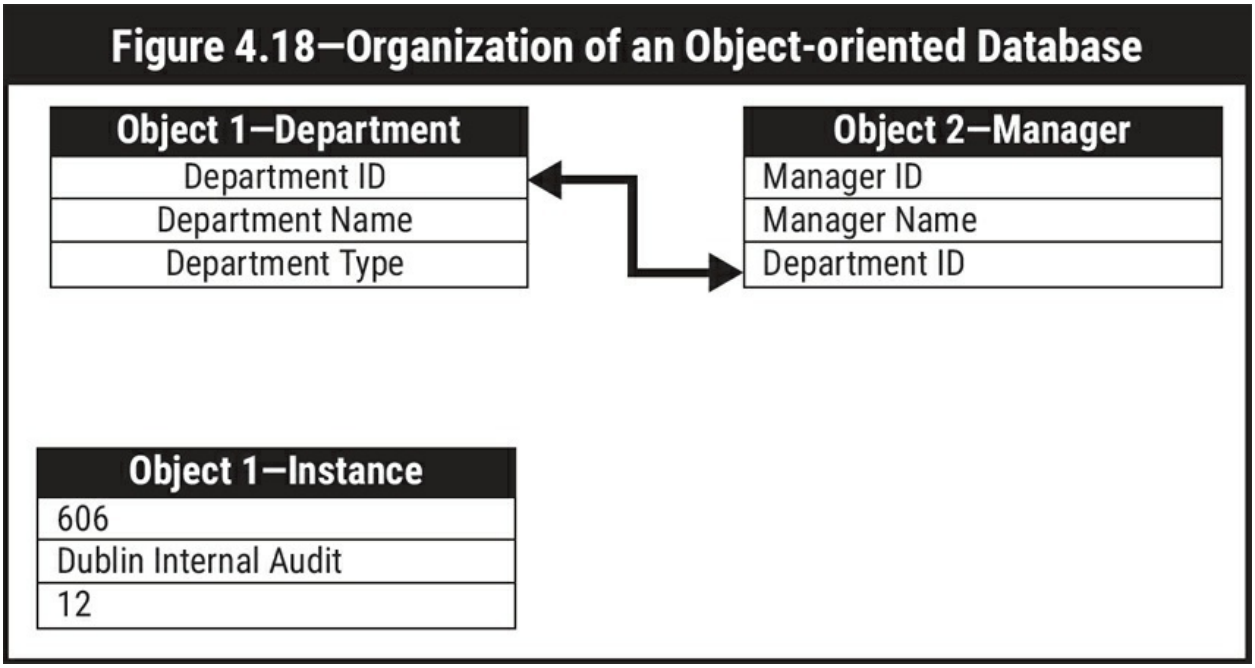
• Each tuple (record) consists of a primary key that identifies some entity, together with a set of zero or more mutually independent attribute values that describes the entity in some way (fully dependent on primary key).

• Any foreign key should have a null value or should have an existing value linking to other tables; this is known as referential integrity.

Object-oriented Database Management System (OODBMS)—An

example of an OODBMS can be seen in **figure 4.18**. In an OODBMS, information is stored as objects (as used in object-oriented programming) rather than data (as in rational databases). This means that all of the features related to object-oriented programming can be applied, including encapsulation (i.e., the creation of data types or classes, including objects) and inheritance (i.e., classes inherit features from other classes). This results in objects that contain both executable code and data. The actual storage of the object in the database is achieved by assigning each object a unique identifier. These are loaded into virtual memory when referenced allowing them to be found quickly. OODBMS

has found a niche in areas such as engineering, science and spatial databases, and is often used when the database is made up of graphics, diagrams or sound that cannot easily be defined or queried by relational databases.



NoSQL—NoSQL databases were developed in response to a rise in the volume of data stored on the Internet commonly known as big data. Much of these data are unstructured audio, video, tweets, logs, blogs, etc. These data cannot be broken out into components, which is required for a relational database; however, NoSQL databases may also support SQL, hence the term

“Not only SQL.” NoSQL databases may support object orientation (as per OODBMS) and other database technologies, shown in **figure 4.19**.

Figure 4.19—NoSQL Database Technologies

Data Model

Description

Key Value

All items in the database are stored as an attribute name (key) with its value.

Column-oriented

All of the values of a column are put together followed by all the values of the next column, then the values of the next column, etc.

Graph Database

Databases based on graph theory (mathematical models of the

relationship between objects)

Document-oriented

Manages, stores and retrieves document-oriented information. This is achieved using storage methods, such as XML and JSON.

The advantages of NoSQL databases include sharding—the ability to

partition the database horizontally across database servers to spread the workload (important when dealing with big data)—and dynamic schemas—

the schema does not have to be defined before you add data (as in relational databases). Common NoSQL databases include MongoDB and Cassandra.

4.11.3 DATABASE CONTROLS

It is critical that database integrity and availability are maintained. This is ensured through the following controls:

• Establish and enforce definition standards.

• Establish and implement data backup and recovery procedures to ensure database availability.

• Establish the necessary levels of access controls, including privileged access, for data items, tables and files to prevent inadvertent or unauthorized access.

• Establish controls to ensure that only authorized personnel can update the database.

• Establish controls to handle concurrent access problems, such as multiple users desiring to update the same data elements at the same time (i.e., transaction commit, locking of records/files).

• Establish controls to ensure accuracy, completeness and consistency of data elements and relationships in the database. It is important that these controls, if possible, be contained in the table/columns definitions. In this way, there is no possibility that these rules will be violated because of programming flaws or through the usage of utilities in manipulating data.

• Use database checkpoints at junctures in the job stream that minimize data loss and recovery efforts to restart processing after a system failure.

• Perform database reorganization to reduce unused disk space and verify defined data relationships.

• Follow database restructuring procedures when making logical, physical and procedural changes.

• Use database performance reporting tools to monitor and maintain database efficiency (e.g., available storage space, buffer size, CPU usage, disk storage configuration and deadlock conditions).

• Minimize the ability to use nonsystem tools or other utilities (i.e., those outside security control, to access the database).

4.11.4 DATABASE REVIEWS

When auditing a database, an IS auditor should review the design, access, administration, interfaces, portability and database supported IS controls, as shown in **figure 4.20.**

Figure 4.20—Database Reviews

Areas to Review

Questions to Consider

• Logical schema

• Do all entities in the entity-relation diagram exist as tables or views?

• Are all relations represented through foreign keys?

• Are constraints specified clearly?

• Are nulls for foreign keys allowed only when they are in

accordance with the cardinality expressed in the entity-relation model?

• Physical schema

• Has allocation of initial and extension space (storage) for tables, logs, indexes and temporary areas been executed based on the

requirements?

• Are indexes by primary key or keys of frequent access present?

• If the database is not normalized, is justification accepted?

• Access time reports

• Are indexes used to minimize access time?

• Have indexes been constructed correctly?

• If open searches not based on indexes are used, are they justified?

• Database security controls

• Are security levels for all users and their roles identified within the database and access rights for all users and/or groups of users

justified?

• Do referential integrity rules exist and are they followed?

• How is a trigger created and when does it fire?

• Is there a system for setting passwords? Does change of passwords exist and is it followed?

• How many users have been given system administrator privileges?

Do these users require the privilege to execute their job function?

• Has an auditing utility been enabled? Are audit trails being

monitored?

• Can database resources be accessed without using DBMS

commands and SQL statements?

• Is system administrator authority granted to job scheduler?

• Are actual passwords embedded into database utility jobs and

scripts?

• Has encryption been enabled where required?

• Are copies of production data authorized?

• Are copies of production data altered or masked to protected

sensitive data?

• Interfaces with other

• Are integrity and confidentiality of data not affected by data import programs/software

and export procedures?

• Have mechanisms and procedures been put in place to ensure the adequate handling of consistency and integrity during concurrent accesses?

• Backup and disaster

• Do backup and disaster recovery procedures exist to ensure the recovery procedures and

reliability and availability of the database?

controls

• Are there technical controls to ensure high availability and/or fast recovery of the database?

• Database-supported IS

• Is access to shared data appropriate?

controls

• Are adequate change procedures utilized to ensure the integrity of the database management software?

• Is data redundancy minimized by the database management

system? Where redundant data exist, is appropriate cross-

referencing maintained within the system’s data dictionary or other documentation?

• Is the integrity of the database management system’s data

dictionary maintained?

• IT asset management

• Has an owner been designated?

• Have we retained a copy of the contracts/SLAs?

• What is the license agreement? Are we in compliance with it?

PART B: BUSINESS RESILIENCE

Business resilience describes an organization's ability to adapt to disruptions and incidents in order to maintain continuous operations and to protect the organization's assets. Most organizations have some degree of DRPs in place for the recovery of IT infrastructure, critical systems and associated data.

However, many organizations have not taken the next step and developed plans for how key business units will function during a period of IT

disruption. CISA candidates should be aware of the components of disaster recovery and business continuity plans, the importance of aligning one with the other, and aligning DRPs and business continuity plans (BCPs) with the organization's goals and risk tolerance. Also of importance are data backup, storage and retention and restoration.

4.12 BUSINESS IMPACT ANALYSIS

Business impact analysis (BIA) is a critical step in developing the business continuity strategy and the subsequent implementation of the risk countermeasures and the BCP in particular.

BIA is used to evaluate the critical processes (and IT components supporting them) and to determine time frames, priorities, resources and

interdependencies. Even if an extensive risk assessment was done prior to BIA, and the criticality and risk are input into BIA, the rule of thumb is to double-check. Often, the BIA uncovers some less visible, but nonetheless vital, component that supports the critical business process. Where IT

activities have been outsourced to third-party service providers, the contractual commitments (in a BCP context) should also be considered.

To perform this phase successfully, one should obtain an understanding of the organization, key business processes and IT resources used by the organization to support the key business processes. Often, this may be obtained from the risk assessment results. BIA requires a high level of senior

management support/sponsorship and extensive involvement of IT and end-user personnel. The criticality of the information resources (e.g., applications, data, networks, system software, facilities) that support an organization's business processes must be approved by senior management.

For the BIA, it is important to include all types of information resources and to look beyond traditional information resources (i.e., database servers).

Information systems consist of multiple components. Some of the

components (e.g., database servers or storage arrays) are quite visible. Other components (e.g., gateways, transport servers, are collected for the BIA from different parts of the organization that own critical processes/applications. To evaluate the impact of downtime for a particular process/application, the impact bands are developed (i.e., high, medium, low) and, for each process, the impact is estimated in time (hours, days, weeks). The same approach is used when estimating the impact of data loss. If necessary, the financial impact may be estimated using the same techniques, assigning the financial value to the particular impact band.

In addition, data for the BIA may be collected on the time frames needed to supply vital resources—how long the organization may run if a supply is broken or when the replacement has arrived. For example, how long will the bank run without plastic cards with chips to be personalized into credit cards or when will IT need to have the desktop workstations shipped in after a disaster?

There are different approaches for performing a BIA. One popular approach is a questionnaire approach, which involves developing a detailed questionnaire and circulating it to key users in IT and end-user areas. The information gathered is tabulated and analyzed. If additional information is required, the BIA team would contact the relevant users for additional information. Another popular approach is to interview groups of key users.

The information gathered during these interview sessions is tabulated and analyzed for developing a detailed BIA plan and strategy. A third approach is to

bring relevant IT personnel and end users (i.e., those owning the critical processes) together in a room to come to a conclusion regarding the potential

business impact of various levels of disruptions. The latter method may be used after all the data are collected. Such a mixed group will quickly decide on the acceptable downtime and vital resources.

Wherever possible, the BCP team should analyze past transaction volume in determining the impact to the business if the system were to be unavailable for an extended period of time. This would substantiate the interview process that the BCP team conducts for performing a BIA.

The three main questions that should be considered during the BIA phase are depicted in **figure 4.21**.

To make decisions, there are two independent cost factors to consider, as shown in **figure 4.22**. One is the downtime cost of the disaster. This component, in the short run (e.g., hours, days and weeks), grows quickly with time, where the impact of a disruption increases the longer it lasts. At a certain moment, it stops growing, reflecting the moment or point when the business can no longer function. The cost of downtime (increasing with time) has many components (depending on the industry and the specific company and circumstances), among them: cost of idle resources (e.g., in production), drop in sales (e.g., orders), financial costs (e.g., not invoicing nor collecting), delays (e.g., procurement) and indirect costs (e.g., loss of market share, image and goodwill).

The other factor is the cost of the alternative corrective measures (i.e., the implementation, maintenance and activation of the BCP). This cost decreases with the target chosen for recovery time. The recovery cost also has many components (most of them rigid-inelastic). This includes the costs of preparing and periodically testing the BCP, offsite backup premises, insurance coverage, alternative site arrangements, etc. The cost of alternative recovery strategies may be plotted as discrete points on the time and cost coordinates and a curve drawn joining the points (**figure 4.22**). The curve as a whole is representative of all possible strategies.

Figure 4.21—Typical Support Functions

1. What are the different business processes? Each process needs to be assessed to determine its relative importance. Indications of criticality include, for

example:

• The process supporting health and safety, such as hospital patient records and air traffic control systems

• Disruption of the process causing a loss of income to the organization or exceptional unacceptable costs

• The process meeting legal or statutory requirements

• The number of business segments or number of users that are affected A process can be critical or noncritical depending on factors such as time of operation and mode of operation (e.g., business hours or ATM operations).

2. What are the critical information resources related to an organization's critical business processes? This is the first consideration because disruption to an information resource is not a disaster in itself, unless it is related to a critical business process (e.g., an organization losing its revenue-generating business processes due to an IS failure).

Other examples of potential critical business processes may include:

• Receiving payments

• Production

• Paying employees

• Advertising

• Dispatching of finished goods

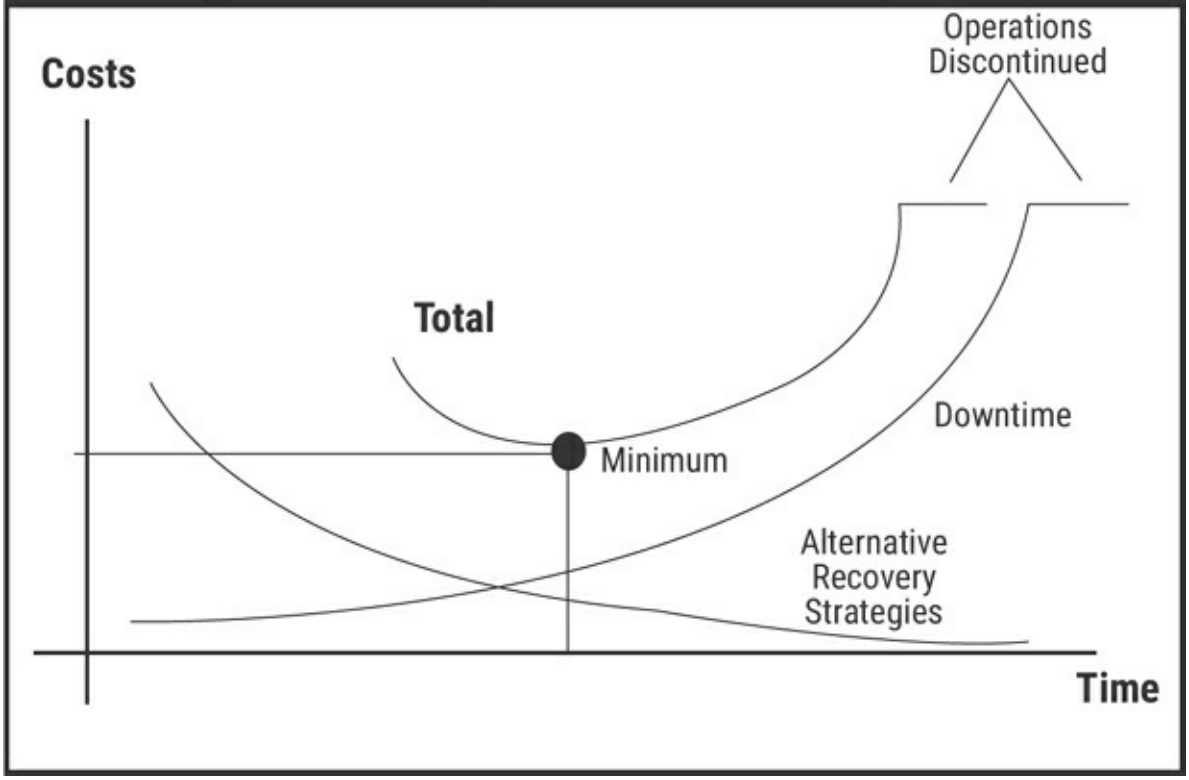
• Legal and regulatory compliance

3. What is the critical recovery time period for information resources in which business processing must be resumed before significant or unacceptable losses are suffered? In large part, the length of the time period for recovery depends on the nature of the business or service being disrupted.

For instance, financial institutions, such as banks and brokerage firms, usually

will have a much shorter critical recovery time period than manufacturing firms. Also, the time of year or day of week may affect the window of time for recovery. For example, a bank experiencing a major outage on Saturday at midnight has a longer time in which to recover than on Monday at midnight, assuming that the bank is not processing on Sunday.

Figure 4.22—Disruption Costs vs. Recovery Costs



Each possible strategy has a fixed-base cost (i.e., does not change with time until an eventual disaster happens). Note that the fixed-base cost of each possible strategy will normally differ. If the business continuity strategy aims at a longer recovery time, it will be less expensive than a more stringent requirement but may be more susceptible to downtime costs spiraling out of control. Normally, the shorter the target recovery time, the higher the fixed cost. The organization pays for the cost of planning and implementation even if no disaster takes place.

If there is a disaster, variable costs will significantly increase (e.g., a warm site contract may consist of a flat annual fee plus a daily fee for actual occupation; extra staff, overtime, transportation and other logistics (e.g., staff *per diem*, new communication lines, etc.) need to be considered. Variable costs will depend on

the strategy implemented.

Having plotted the two curves—downtime costs and costs of alternative

recovery strategies—**figure 4.22** shows the curve of total cost (the sum of the other two cost curves). An organization would choose the point at which those total costs are minimal.

In summary, the sum of all costs—downtime and recovery—should be minimized. The first group (downtime costs) increases with time, and the second (recovery costs) decreases with time; the sum usually is a U curve. At the bottom of the U curve, the lowest cost can be found.

Note: The CISA candidate will not be tested on calculations of costs.

4.12.1 CLASSIFICATION OF OPERATIONS AND CRITICALITY ANALYSIS

A system's risk ranking involves a determination of risk that is based on the impact derived from the critical recovery time period and the likelihood that an adverse disruption will occur. Many organizations use a risk of occurrence to determine a reasonable cost of being prepared. For example, they may determine that there is a 0.1 percent risk (or 1 in 1,000) that over the next five years the organization will suffer a serious disruption. If the assessed impact of a disruption is US $10 million, then the maximum reasonable cost of being prepared might be US $10 million × 0.1 percent = US $10,000 over five years. Such a method is called the annual loss expectancy (ALE). From this risk-based analysis process, prioritizing critical systems can take place in developing recovery strategies. The risk ranking procedure should be performed in coordination with IS processing and end-user personnel.

A typical risk ranking system may contain the classifications as found in

figure 4.23.

Figure 4.23—Classification of Systems

Classification

Description

Critical

These functions cannot be performed unless they are replaced by

identical capabilities. Critical applications cannot be replaced by manual methods. Tolerance to interruption is very low; therefore, cost

of interruption is very high.

Vital

These functions can be performed manually, but only for a brief

period of time. There is a higher tolerance to interruption than with critical systems and, therefore, somewhat lower costs of interruption, provided that functions are restored within a certain time frame (usually five days or less).

Sensitive

These functions can be performed manually, at a tolerable cost and for an extended period of time. While they can be performed

manually, it usually is a difficult process and requires additional staff to perform.

Nonsensitive

These functions may be interrupted for an extended period of time, at little or no cost to the company, and require little or no catching up when restored.

The next phase in continuity management is to identify the various recovery strategies and available alternatives for recovering from an interruption and/or disaster. The selection of an appropriate strategy that is based on the BIA and criticality analysis is the next step for developing BCPs and DRPs.

The two metrics that help in determining the recovery strategies are the recovery point objective (RPO) and recovery time objective (RTO). For additional information on RPO and RTO, see section 4.16 Disaster Recovery Plans.

4.13 SYSTEM RESILIENCY

System resilience is the ability of a system to withstand a major disruption within set metrics and recovery times. This can include the ability to maintain capability during the disruption.

4.13.1 APPLICATION RESILIENCY AND DISASTER

RECOVERY METHODS

Protecting an application against a disaster entails providing a way to restore it as quickly as possible. Clustering makes it possible to do so. A cluster is a type of software (agent) that is installed on every server (node) in which the application runs and includes management software that permits control of and tuning the cluster behavior. Clustering protects against single points of failure (a resource whose loss would result in the loss of service or

production). The main purpose of clustering is higher availability.

There are two major types of application clusters: active-passive and active-active. In active-passive clusters, the application runs on only one (active) node, while other (passive) nodes are used only if the application fails on the active node. In this case, cluster agents constantly watch the protected application and quickly restart it on one of the remaining nodes. This type of cluster does not require any special setup from the application side (i.e., the application does not need to be cluster-aware). Hence, it is one of the major ways to ensure application availability and disaster recovery. In active-active clusters, the application runs on every node of the cluster. With this setup, cluster agents coordinate the information processing between all of the nodes, providing load balancing and coordinating concurrent data access. When an application in such a cluster fails, users normally do not experience any downtime at all (possibly missing uncompleted transactions). Active-active clusters require that the application be built to utilize the cluster capabilities (for instance, if the transaction is not completed on the node that failed, some other remaining node will try to rerun the transaction). Such clusters are less common than active-passive and provide quick application recovery, load balancing and scalability. This type of cluster puts a greater demand on network latency. Very often, organizations use a combination of cluster setups; for instance, active-active for a particular processing site and active-passive between the sites. This combination protects applications against local software or hardware failure (active-active) and against site failure (active-passive). The clusters with a span

of one city are called metro-clusters, while clusters spanning between cities, countries and continents are called geo-clusters.

Although it is possible to develop cluster software in-house, generally, it is not economically viable, and there are a number of solutions available from major software vendors. Often, clustered applications require that the data are shared between all nodes of the cluster. Active-active clusters generally require that the same storage be available to all of the nodes; active-passive clusters are less demanding and require that the data are replicated from the active node to others.

4.13.2 TELECOMMUNICATION NETWORKS

RESILIENCY AND DISASTER RECOVERY METHODS

The plan should contain the organization's telecommunication networks.

Today, telecommunication networks are key to business processes in large and small organizations; therefore, the procedures to ensure continuous telecommunication capabilities should be given a high priority.

Telecommunication networks are susceptible to the same natural disasters as data centers but also are vulnerable to several disastrous events unique to telecommunications. These include central switching office disasters, cable cuts, communication software glitches and errors, security breaches connected to hacking (phone hackers are known as phreakers), and a host of other human mishaps. It is the responsibility of the organization and not the local exchange carriers to ensure constant communication capabilities. The local exchange carrier is not responsible for providing backup services, although many do back up main components within their systems. Therefore, the organization should make provisions for backing up its own

telecommunication facilities.

To maintain critical business processes, the information processing facility's (IPF) BCP should provide for adequate telecommunications capabilities.

Telecommunications capabilities to consider include telephone voice circuits, WANs (connections to distributed data centers), LANs (work group PC

connections), and third-party EDI providers. The critical capacity requirements

should be identified for the various thresholds of outage for each telecommunications capability, such as two hours, eight hours or 24

hours. Uninterruptible power supplies (UPSs) should be sufficient to provide backup to the telecommunication equipment as well as the computer equipment.

Methods for network protection are:

• **Redundancy**—This involves a variety of solutions, including: – Providing extra capacity with a plan to use the surplus capacity if the normal primary transmission capability is not available. For a LAN, a second cable can be installed through an alternate route for use if the primary cable is damaged.

– Providing multiple paths between routers

– Using dynamic routing protocols, such as Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP)

– Providing for failover devices to avoid single point of failures in routers, switches, firewalls, etc.

– Saving configuration files for recovery if network devices, such as those for routers and switches, fail. For example, organizations should use Trivial File Transport Protocol (TFTP) servers. Most network devices support TFTP for saving and retrieving configuration information.

• **Alternative routing**—The method of routing information via an alternate medium, such as copper cable or fiber optics. This method uses different networks, circuits or end points if the normal network is unavailable. Most local carriers are deploying counter-rotating, fiber-optic rings. These rings have fiber-optic cables that transmit information in two different directions and in separate cable sheaths for increased protection. Currently, these rings connect through one central switching office. However, future expansion of the rings may incorporate a second central office in the circuit. Some carriers are offering alternate routes to different points of presence or alternate central offices. Other examples include a dial-up circuit as an alternative to dedicated circuits, cellular phone and microwave communication as alternatives to land circuits, and couriers as an alternative to electronic transmissions.

• **Diverse routing**—The method of routing traffic through split cable facilities or

duplicate cable facilities, with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. However, acquiring this type of access is time consuming and costly. Most carriers provide facilities for alternate and diverse routing, although the majority of services are transmitted over terrestrial media. These cable facilities are usually located in the ground or basement. Ground-based facilities are at great risk due to the aging infrastructures of cities. In addition, cable-based facilities usually share a room with mechanical and electrical systems that can impose great risk due

to human error and disastrous events.

• **Long-haul network diversity**—Many vendors of recovery facilities have provided diverse long-distance network availability, using T1 circuits among the major long-distance carriers. This ensures long-distance access if any single carrier experiences a network failure. Several of the major carriers now have installed automatic rerouting software and redundant lines that provide instantaneous recovery if a break in their lines occurs.

The IS auditor should verify that the recovery facility has these vital telecommunications capabilities.

• **Last-mile circuit protection**—Many recovery facilities provide a redundant combination of local carrier T1s or E1s, microwave, and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster.

Alternate local carrier routing also is used.

• **Voice recovery**—With many service, financial and retail industries dependent on voice communication, redundant cabling and VoIP are common approaches to deal with it.

4.14 DATA BACKUP, STORAGE AND RESTORATION

Because data are key assets to any organization, data backup, storage and

potential restoration are key considerations for the enterprise. Laws and regulations may impact how an enterprise can handle this data and should be considered in developing methods for data handling.

4.14.1 DATA STORAGE RESILIENCY AND DISASTER RECOVERY METHODS

Redundant Array of Independent (or Inexpensive) Disks (RAID) is the most common, basic way to protect data against a single point of failure, in this instance, a disk failure. RAID provides performance improvements and fault-tolerant capabilities via hardware or software solutions, breaking up data and writing data to a series of multiple disks to simultaneously improve performance and/or save large files. These systems provide the potential for cost-effective mirroring offsite for data backup. A variety of methods, categorized into 11 levels (the most popular being 0 [stripe], 1 [mirror], their

combinations [0+1 or 1+0] and 5), is defined for combining several disk drives into what appears to the system as a single disk drive. RAID improves on the single-drive-only solution, because it offers better performance and/or data redundancy.

Note: The CISA candidate will not be tested on the specifics of RAID

levels.

Many vendors offer storage arrays—hardware that hides all the complexities of forming logical volumes from physical disks, thus completely removing the need for the low-level configuration. Typically, these storage arrays provide major RAID levels; however, that does not remove the need for responsible IT staff to understand the implications of the different RAID

configurations.

To protect data against site failure and to ensure successful application recovery (with or without clusters), storage arrays provide data replication features, making sure that what data are saved to the disk on one site appear on the other site. Depending on the available network bandwidth and latency, this data replication may be synchronous (i.e., the local disk write is not confirmed until the data are written to the disk on the other site), asynchronous (data are

replicated on a schedule basis) or adaptive (switching from one mode to another depending upon the network load).

The array-based (hardware) replication is absolutely transparent to the application (i.e., no special provisions are needed from the OS or the application side).

If there is no disk array, the data stored on local server volumes (RAID or not) can still be replicated to a remote site by using host-based data replication solutions. These act similarly to hardware-based solutions.

4.14.2 BACKUP AND RESTORATION

To ensure that the critical activities of an organization (and supporting applications) are not interrupted in the event of a disaster, secondary storage

media are used to store software application files and associated data for backup purposes. These secondary storage media are removable media (tape cartridges, CDs, DVDs) or mirrored disks (local or remote) or network storage. Typically, the removable media are recorded in one facility and stored in one or more remote physical facilities (referred to as offsite libraries). The number and locations of these remote storage facilities are based on availability of use and perceived business interruption risk.

Maintaining the inventory (catalog) of the remote storage facility can be performed automatically (vaulting solutions) or manually. In the latter case, it is the offsite librarian’s responsibility to maintain a continuous inventory of the contents of these libraries, to control access to library media and to rotate media between various libraries, as needed. As the amount of information increases, keeping manual inventories of tape backups (whether local or remote) becomes increasingly difficult and is gradually being replaced by integrated backup and recovery solutions that handle the backup catalogs—

remote and local.

Offsite Library Controls

When disaster strikes, the offsite storage library often becomes the only remaining copy of the organization’s data. To ensure that these data are not lost, it is very important to implement strict controls over the data—both physical and

logical. Unauthorized access, loss or tampering with this information (either onsite or while in transit) could impact the information system's ability to provide support for critical business processes, putting the very future of the organization at risk.

Controls over the offsite storage library include:

• Secure physical access to library contents, ensuring that only authorized personnel have access.

• Encrypt backup media especially when they are in transit.

• Ensure that physical construction can withstand fire/heat/water.

• Locate the library away from the data center, preferably in a facility that will not be subject to the same disaster event, to avoid the risk of a disaster affecting both facilities.

• Ensure that an inventory of all storage media and files stored in the library is maintained for the specified retention time.

• Ensure that a record of all storage media and files moved into and out of the library is maintained for the specified retention/expiration time.

• Ensure that a catalog of information regarding the versions and location of data files is maintained for the specified retention time and protecting this catalog against unauthorized disclosure.

The retention time for the different records must be in accordance with the enterprise retention policy.

Security and Control of Offsite Facilities

The offsite IPF must be as secured and controlled as the originating site. This includes adequate physical access controls, such as locked doors, no windows and active surveillance. The offsite facility should not be easily identified from the outside. This is to prevent intentional sabotage of the offsite facility should the destruction of the originating site be from a malicious attack. The offsite facility should not be subject to the same disaster event that affected the originating site.

The offsite facility should possess at least the same constant environmental monitoring and control as the originating site, or the ones that are dictated by business requirements. This includes monitoring the humidity, temperature and surrounding air to achieve the optimum conditions for storing optical and magnetic media, and, if applicable, servers, workstations, storage arrays and tape libraries. The proper environmental controls include a UPS, operating on a raised floor with proper smoke and water detectors installed, climate controls and monitoring for temperature and humidity, and a working/tested fire extinguishing system. Provisions for paper record storage should ensure that a fire hazard is not created. Additional controls should be implemented in case of specific legal, regulatory or business requirements.

Media and Documentation Backup

A crucial element of a DRP (on- or offsite) is the availability of adequate data. Duplication of important data and documentation, including offsite storage of such backup data and paper records, is a prerequisite for any type of recovery.

Where information is processed and stored in a confidential environment at the primary site and backup is to be stored in a similarly secure location, care should be exercised to ensure that the means of transporting data, whether in the form of physical backup media or via mirrored backups on the network, extend adequate protection to the information.

Types of Backup Devices and Media

The backup device and media must be chosen based on a variety of factors:

• **Standardization**—Very specific technologies require a lot of support for both the primary site and the offsite facility, increasing costs.

• **Capacity**—Backup media should have adequate capacity, in order to reduce the number of media necessary to implement a backup set.

• **Speed**—Processes to backup and restore should be completed in an acceptable time, to comply with business requirements.

• **Price**—Backup devices are only part of the costs; attention must be paid to media prices.

There are a lot of different devices and media types available. The technology chosen must be adequate to the business needs. **Figure 4.24** provides some examples.

Figure 4.24—Types of Media

Portability

Small Amounts, Few

Large Amounts, Frequent Changes

Changes

Removable media

CDs, DVDs, removable

Tape-based backup systems (DDS,

hard drives or solid-state

digital audio tape [DAT], DLT, AIT,

drives

LTO)

Nonremovable media

Disk-based backup (virtual tape

libraries [VTLs]), disk snapshots,

host-based or disk-array-based

replication

Modern tape-based backup systems are libraries with up to hundreds of tape drives and up to several thousands of tape slots. These libraries may be equipped with robotic arms and barcode scanners. Barcode scanners are used to quickly

determine the contents of backup tapes. Without a barcode

scanner, the tape must be actually inserted into tape drive and its header must be read and compared to backup catalog to read the tape contents. Having a barcode scanner makes this process quicker—the backup catalog contains the tape numbers written on the barcode instead of reading it in the drive. The robotic arms make the process of scanning the barcode and transporting the tape to the tape drive significantly faster. Tape libraries are controlled by backup and recovery applications which are available from major software companies. These applications:

• Handle backup and recovery tasks according to backup and recovery policies

• Maintain backup catalog (local and remote)

• Control tape libraries

The most important feature of the tape drives is its data interface. Modern tape drives have fiber channel (FC) or serial attached SCSI (SAS) interfaces, conventional parallel SCSI is gradually coming out of use. Tape libraries are connected either to SAN (via FC) or attached to backup and recovery server through SAS or iSCSI connections. Typically, tape libraries have LAN

interfaces for maintenance and diagnostics.

Disk-based backup systems exist in different types:

• **Virtual tape libraries (VTLs)**—These systems consist of disk storage (typically mid-range disk arrays) and software that control backup and recovery data sets. For an external user (backup and recovery software), VTLs behave like a conventional tape library; however, data are stored on a disk array. Often, for the disaster recovery purposes the contents of a VTL are replicated from primary site to a backup site using the hardware-based replication provided by a disk array.

• **Host-based replication**—This replication is executed at the host (server) level by a special software running on this server and on the target server.

It can occur in real-time (synchronous mode, the data are not written to the primary site until the backup site sends the confirmation the replicated data have

arrived and safely written to the disk) or with some delay

(asynchronous mode, when data are transferred to the backup site with some delay). The software packages are available from major software vendors.

• **Disk-array-based replication**—The same as host-based replications, however the replication is performed at the disk array level, completely hidden from servers and applications. This feature is available from all major hardware vendors supplying mid-range and high-end disk arrays.

The replication can be completed via SAN or LAN.

• **Snapshots**—This technology is very flexible, allowing making different types of momentary copies of volumes or file systems. Depending upon types of snapshots, either full copy is created each time or only the changed blocks of data or files are stored. This technology is especially efficient and effective while used in combination with backup and recovery software.

For instance, a snapshot is taken and then mounted on a different server, full backup is performed, thus saving the production system from overhead load. Another example is replicating data to remote site, making snapshots on the remote site and using them for backup and recovery, thus using the server equipment at the backup site.

In an environment where server virtualization is used, disk-based backup systems can provide an excellent disaster recovery solution because entire virtual servers may be replicated to the recovery site.

Copies of data taken for offsite backup must be given the same level of security as the original files. The offsite facility and transportation arrangements must, therefore, meet the security requirements for the most sensitive class of data on the backup media.

Periodic Backup Procedures

Both data and software files should be backed up on a periodic basis in accordance with the defined RPO. The time period in which to schedule the backup may differ per application program or software system. For instance, the locations (folders or volumes) where the application data are stored must be backed up regularly since the data are frequently changed by daily transactions.

The locations where application configuration and software files (application or OS) are stored are updated less frequently—only when the configurations change or a patch is applied. Often, online/real-time systems that perform large-volume transaction processing require nightly or hourly backups or use data replication at a separate remote processing facility.

Scheduling the periodic backups can often be easily accomplished via an automated backup/media management system and automated job scheduling software. Using the integrated solution for backup/recovery procedures and media management will prevent erroneous or missed backup cycles due to operator error. Schedules describing backup of certain data are included in the backup procedures.

Modern backup and recovery solutions include special pieces of software called “agents” that are installed on the protected servers and workstations.

These agents are collecting the data (data files, configuration files, software application files) and shipping them to the backup and recovery server(s) that convert data for subsequent storage on tape or disk. The same agents are used for data restoration.

Frequency of Rotation

Backup for data and software must allow for the continuing occurrence of change. A copy of the file or record, as of some point in time, is retained for backup purposes. All changes or transactions that occur during the interval between the copy and the current time also are retained.

Considerations for establishing file backup schedules include the following:

• The frequency of backup cycle and depth-of-retention generations must be determined for each application.

• The backup procedures must anticipate failure at any step of the processing cycle.

• For legacy systems, master files should be retained at appropriate intervals, such as at the end of an updating procedure, to provide synchronization between files and systems.

• Transaction files should be presented to coincide with master files so a prior generation of a master file can be brought completely up-to-date to recreate a current master file.

• DBMS require specialized backup, usually provided as an integral feature of the DBMS or the special part of the backup and recovery software (agent) designed especially for the particular make and version of the database.

• It may be necessary to secure the license to use certain vendor software at

an alternate site; this should be arranged in advance of the need.

• Backup for custom-built software must include object-code and source-code libraries and provisions for maintaining program patches on a current basis at all backup locations.

• Backup hardware should be available at the offsite facility and should be compatible with backup media. Also, for long-term retention, it is necessary to have technical support and maintenance agreements to guarantee that the alternate backup hardware will work properly in case of restoration.

Likewise, any documentation required for the consistent and continual operation of the business should be preserved in an offsite backup facility.

This includes source documents required for restoration of the production database. As with data files, the offsite copies should be kept up to date to ensure their usefulness. It is important to remember that adequate backup is a prerequisite to successful recovery.

Types of Media and Documentation Rotated

Without software, the computer hardware is of little value. Software, including OSs, programming languages, compilers, utilities and application programs, along with copies of paper documentation—such as operational guides, users manuals, records, data files, databases, etc.—should be maintained and stored offsite in their current status. This information provides the raw materials and finished products for the IS processing cycle and should be stored offsite.

Figure 4.25 describes the documentation to be backed up and stored offsite.

Figure 4.25—Offsite Storage

Classification	Description
Operating procedures	Application run books, job stream control instructions, OS manuals and special procedures
System and program	Flow charts, program source code listings, program logic
documentation	descriptions, statements, error conditions and user manuals
Special procedures	Any procedures or instructions that are out of the ordinary, such as
exception processing, variations in processing and emergency processing	
Input source documents,	Duplicate copies, photocopies, microfiche, microfilm reports or
output documents	summaries required for auditing, historical analysis, performance of vital work, satisfaction of legal requirements or expediting insurance claims
Business continuity plan	A copy of the correct plan for reference

Sensitive data that are stored offsite should be stored in a fire-resistant magnetic media container. When the data are shipped back to the recovery site, the data should be stored and sealed in the magnetic media container.

Every organization should have a written policy to govern what is stored and for how long. Backup schedules and rotation media to be used in an offsite location are important. This rotation of media can be performed via management software.

4.14.3 BACKUP SCHEMES

There are three main schemes for backup: full, incremental and differential.

Each one has its advantages and disadvantages. Usually, the methods are combined, in order to complement each other.

Full Backup

This type of backup scheme copies all files and folders to the backup media, creating one backup set (with one or more media, depending on media capacity). The main advantage is having a unique repository in case of restoration, but it requires more time and media capacity.

Incremental Backup

An incremental backup copies the files and folders that changed or are new since the last incremental or full backup. If you have a full backup on day 1, your incremental backup on day 2 will copy only the changes from day 1 to day 2. On day 3, it will copy only the changes from day 2 to day 3, and so on.

Incremental backup is a faster method of backup and requires less media capacity, but it requires that all backup sets restore all changes since a full backup, and restoration will take more time. **Figure 4.26** provides an

Figure 4.26—Full Plus Incremental Backup Scheme

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
File 1	x	x					
File 2	x		x				
File 3	x			x			
File 4	x				x		

example of a full plus incremental backup scheme. On day 1 there was a full backup and all files were saved to backup media. On days 2 to 7, there were incremental backups. On day 2, file 1 changed. On day 3, file 2 changed. On day 4, file 3 changed. On day 5, file 4 changed. The X shows which files were backed up.

Differential Backup

A differential backup copies all files and folders that have been added or changed since a full backup was performed. This type of backup is faster and requires less media capacity than a full backup and requires only the last full and differential backup sets to make a full restoration. It also requires less time to restore than incremental backups, but it is slower and requires more media capacity than incremental backups because data that are backed up are cumulative.

Figure 4.27 depicts an example of a full plus differential backup scheme. On day 1 there is a full backup. On days 2 to 7, there are differential backups. On day 2, file 1 changed. On day 3, file 2 changed. On day 4, file 3 changed. On day 5, file 4 changed. The X shows which files were backed up.

Note that, in differential backups, all files or folders that were changed since a full backup are repeatedly copied to the backup media.

Figure 4.27—Full Plus Differential Backup Scheme

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
File 1	x	x	x	x	x		
File 2	x		x	x	x		
File 3	x			x	x		
File 4	x				x		

Method of Rotation

Although there are various approaches for the rotation of media, one of the more accepted techniques is referred to as the Grandfather-Father-Son method. In this method, daily backups (son) are made over the course of a week. The final

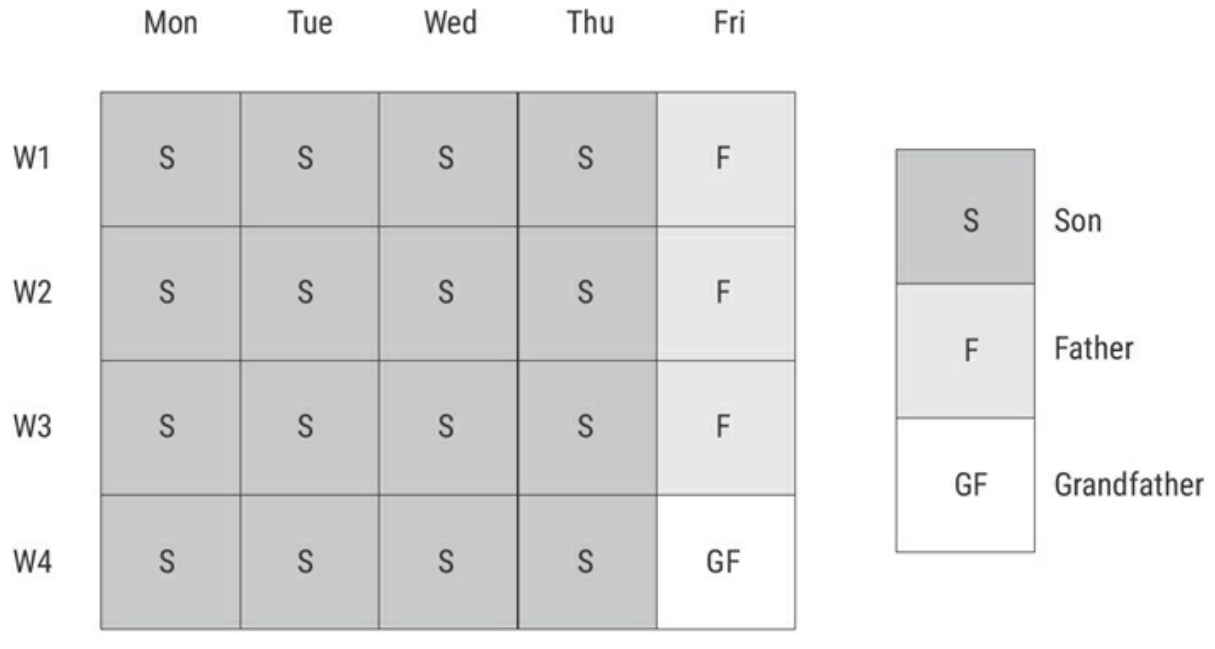
backup taken during the week becomes the backup for that week (father). The earlier daily backup media are then rotated for reuse as backup media for the second week. At the end of the month, the final weekly backup is retained as the backup for that month (grandfather). Earlier weekly backup media are then rotated for reuse in subsequent months. At the end of the year, the final monthly backup becomes the yearly backup. Normally, monthly and annual tapes/other media are retained and not subject to the rotation cycle. See **figures 4.28** and **4.29** for examples of typical rotation cycles. Testing all aspects of the DRP is the most important factor in achieving success in an emergency situation. The main objective of testing is to ensure that executing the plans will result in the successful recovery of the infrastructure and critical business processes. Testing should focus on:

- Identifying gaps
- Verifying assumptions
- Testing time lines
- Effectiveness of strategies
- Performance of personnel
- Accuracy and currency of plan information

Figure 4.28—Typical Rotation Cycle, Sample A

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
Week 1	Tape 1	Tape 2	Tape 3	Tape 4	Tape 5	Tape 6	Tape 7 (week tape)
Week 2	Tape 1	Tape 2	Tape 3	Tape 4	Tape 5	Tape 6	Tape 8 (week tape)
Week 3	Tape 1	Tape 2	Tape 3	Tape 4	Tape 5	Tape 6	Tape 9 (week tape)
Week 4	Tape 1	Tape 2	Tape 3	Tape 4	Tape 5	Tape 6	Tape 10 (week tape)
Week 5	Tape 1	Tape 2	Tape 3	Tape 4	Tape 5	Tape 6	Tape 7 (week tape)

Figure 4.29—Typical Rotation Cycle Sample B



Testing promotes collaboration and coordination among teams and is a useful

training tool. Many organizations require complete testing annually. In addition, testing should be considered on the completion or major revision of each draft plan or complementary plans and following changes in key personnel, technology or the business/regulatory environment.

Testing must be carefully planned and controlled to avoid placing the business at increased risk. To ensure that all plans are regularly tested, the IS

auditor should be aware of the testing schedule and tests to be conducted for all critical functions.

All tests must be fully documented with pretest, test and posttest reports. Test documentation should be reviewed by the IS auditor. Information security should also be validated during the test to ensure that it is not being compromised. A key element to this approach is that backups rotated offsite should not be returned for reuse until their replacement has been sent offsite.

As an example, the backup media for week 1 should not be returned from offsite storage until the month-end backup is safely stored offsite. Variations of this method can be used depending on whether quarterly backups are required and on the amount of redundancy an organization may wish to have.

Record Keeping for Offsite Storage

An inventory of contents at the offsite storage location should be maintained.

This inventory should contain information such as:

• Data set name, volume serial number, date created, accounting period and offsite storage bin number for all backup media

• Document name, location, pertinent system and date of last update for all critical documentation

Automated media management systems usually have options that help in recording and maintaining this information—bar code stickers for magnetic tapes and robotic arms with bar code readers for tape libraries. If backup media are carried between facilities, then both receipt and shipment logs should be maintained to assist tracking in case of losses.

4.15 BUSINESS CONTINUITY PLAN

The purpose of business continuity/disaster recovery is to enable a business to continue offering critical services in the event of a disruption and to survive a disastrous interruption to activities. Rigorous planning and commitment of resources is necessary to adequately plan for such an event.

The first step in preparing a new BCP, or in updating an existing one, is to identify the business processes of strategic importance—those key processes that are responsible for both the permanent growth of the business and for the fulfillment of the business goals. Ideally, the BCP/DRP should be supported by a formal executive policy that states the organization's overall target for recovery and empowers those people involved in developing, testing and maintaining the plans.

Based on the key processes, the risk management process should begin with a risk assessment. The risk is directly proportional to the impact on the organization and the probability of occurrence of the perceived threat. Thus, the result of the risk assessment should be the identification of the following:

• Human resources, data, infrastructure elements and other resources (including those provided by third parties) that support the key processes

• List of potential vulnerabilities—the dangers or threats to the organization

• Estimated probability of the occurrence of these threats

• Efficiency and effectiveness of existing risk mitigation controls (risk countermeasures)

BCP is primarily the responsibility of senior management, as they are entrusted with safeguarding the assets and the viability of the organization, as defined in the BCP/DRP policy. The BCP is generally followed by the business and supporting units, to provide a reduced but sufficient level of functionality in the business operations immediately after encountering an interruption, while recovery is taking place. The plan should address all functions and assets required to continue as a viable organization. This includes continuity procedures determined necessary to survive and minimize the consequences of business interruption.

BCP takes into consideration:

• Those critical operations that are necessary to the survival of the

organization

• The human/material resources supporting them

In addition to the plan for the continuity of operations, the BCP includes:

• The DRP that is used to recover a facility rendered inoperable, including relocating operations into a new location

• The restoration plan that is used to return operations to normality whether in a restored or new facility

Depending on the complexity of the organization, there could be one or more plans to address the various aspects of business continuity and disaster recovery. These plans do not necessarily have to be integrated into one single plan. However, each has to be consistent with other plans to have a viable BCP strategy.

It is highly desirable to have a single integrated plan to ensure that:

• There is proper coordination among various plan components.

• Resources committed are used in the most effective way, and there is reasonable confidence that, through its application, the organization will survive a disruption.

Even if similar processes of the same organization are handled at a different geographic location, the BCP and DRP solutions may be different for different scenarios. Solutions may be different due to contractual requirements (e.g., the same organization is processing an online transaction for one client and the back office is processing for another client. A BCP

solution for the online service will be significantly different than one for the back office processing.)

4.15.1 IT BUSINESS CONTINUITY PLANNING

IT business continuity planning uses the same approach as enterprise business continuity planning, except that the continuity of IT processing is threatened. IT processing is of strategic importance—it is a critical component, because most key business processes depend on the availability of key systems infrastructure components and data.

The IT BCP should be aligned with the strategy of the organization. The criticality of the various application systems deployed in the organization depends on the nature of the business as well as the value of each application to the business.

The value of each application to the business is directly proportional to the role of the information system in supporting the strategy of the organization.

The components of the information system (including the technology infrastructure components) are then matched to the applications (e.g., the value of a computer or a network is determined by the importance of the application system that uses it).

Therefore, the information system BCP/DRP is a major component of an organization's overall business continuity and disaster recovery strategy. If the IT plan is a separate plan, it must be consistent with and support the corporate BCP. Throughout the IT business continuity (sometimes referred to as IT service continuity) planning process, the overall BCP of the organization should be taken into consideration; again, this should be supported by the executive policy. All IT plans must be consistent with and support the corporate BCP. This means that alternate processing facilities that support key operations must be ready, be compatible with the original processing facility and have up-to-date plans regarding their use.

Again, all possible steps must be taken to reduce or remove the likelihood of a disruption using the method described in other sections of this manual.

Examples include:

• Minimize threats to the data center by considering location:

– Not on a flood plain

– Not on or near an earthquake fault line

– Not close to an area where explosive devices or toxic materials are regularly used

• Make use of resilient network topographies, such as Loop or Mesh with alternative processing facilities already built into the network infrastructure.

Developing and testing an information system BCP/DRP is a major

component of an organization's overall business continuity and disaster recovery strategy. The plan is based on the coordinated use of whatever risk countermeasures are available for the organization (i.e., duplicate processing facility, redundant data networks, resilient hardware, backup and recovery systems, data replication, etc.). If the IT plan is a separate plan (or multiple separate plans), it must be consistent with and support the corporate BCP.

Establishing dependencies among critical business processes, applications, the information system and IT infrastructure components is a subject of risk assessment. The resulting dependencies map with threats to and

vulnerabilities of the components/dependencies (along with the key applications grouped by their criticality) is the outcome of the risk assessment.

After the risk assessment identifies the importance of the IS components to the organization, and the threats to and vulnerabilities of those components, a remedial action plan can be developed for establishing the most appropriate methods to protect the components. There is always a choice of risk mitigation measures (risk countermeasures)—either to remove the threat and/or fix the vulnerability.

The risk can be either estimated in a qualitative way (assigning qualitative values to the impact of the threat and its probability) or calculated in a quantitative way (assigning a monetary value to the impact [i.e., loss] and assigning a probability).

Note: The CISA candidate will not be tested on the actual calculation of risk analysis; however, the IS auditor should be familiar with risk analysis calculation.

If the organization is willing to investigate the extent of the losses that the business will suffer from the disruption, the organization may conduct a BIA,

which is discussed in section 4.12 Business Impact Analysis. The BIA allows the organization to determine the maximum downtime possible for a particular application and how much data could be lost. The BIA also allows

the organization to quantify the losses as they grow after the disruption, thus allowing the organization to decide on the technology (and facilities) used for protection and recovery of its key information assets (information system, IT

components, data, etc.).

The results of risk assessment and BIA are fed into the IS business continuity strategy, which outlines the main technology and principles behind IT

protection and recovery as well as the road map to implement the technology and principles.

As the IT business continuity strategy and its overarching IT strategy are executed, the IT infrastructure of the organization changes. New risk countermeasures are introduced and old ones become obsolete. The information system BCP must be changed accordingly and retested

periodically to ensure that these changes are satisfactory.

Similar to any BCP, an information system BCP is much more than just a plan for information systems. A BCP identifies what the business will do in the event of a disaster. For example, where will employees report to work, how will orders be taken while the computer system is being restored, which vendors should be called to provide needed supplies? A subcomponent of the BCP is the IT DRP. This typically details the process that IT personnel will use to restore the computer systems, communications, applications and their data. DRPs may be included in the BCP or as a separate document altogether, depending on the needs of the business.

Not all systems will require a recovery strategy. An overriding factor when determining recovery options is that the cost should never exceed the benefit (this usually becomes clear after completing a BIA). One of the important outcomes of BIA, apart from the RTO and RPO, is a way to group

information systems according to their recovery time. This usually guides the selection of the technological solutions (i.e., controls) supporting business

continuity and IT disaster recovery.

The IT disaster recovery usually happens in unusual, stressful circumstances (e.g., fire, flood, hurricane devastation). Often, the security controls (both

physical and IS) may not be functioning. It is, therefore, recommended that the organization implement an information security management system (ISMS) to maintain the integrity, confidentiality and availability of IS, and not only under normal conditions.

4.15.2 DISASTERS AND OTHER DISRUPTIVE EVENTS

Disasters are disruptions that cause critical information resources to be inoperative for a period of time, adversely impacting organizational operations. The disruption could be a few minutes to several months, depending on the extent of damage to the information resource. Most important, disasters require recovery efforts to restore operational status.

A disaster may be caused by natural calamities—such as earthquakes, floods, tornados, severe thunderstorms and fire—which cause extensive damage to the processing facility and the locality in general. Other disastrous events causing disruptions may occur when expected services—such as electrical power, telecommunications, natural gas supply or other delivery services—

are no longer supplied to the company due to a natural disaster or other cause.

Not all critical disruptions in service or disasters are due to natural causes. A disaster could also be caused by events precipitated by human beings, such as terrorist attacks, hacker attacks, viruses or human error. Disruption in service is sometimes caused by system malfunctions, accidental file deletions, untested application releases, loss of backup, network denial of service (DoS) attacks, intrusions and viruses. These events may require action to recover operational status in order to resume service. Such actions may necessitate restoration of hardware, software or data files.

Many disruptions start as minor incidents. Normally, if the organization has a help desk, it would act as the early warning system to recognize the first signs of an upcoming disruption. Often, such disruptions (e.g., gradually deteriorating database performance) go undetected. Until these “creeping disasters” strike (the database halts), they cause only infrequent user complaints.

Based on risk assessment, worst-case scenarios and short- and long-term

fallback strategies are formulated in the IS business continuity strategy for later incorporation into the BCP (or other plan). In the short term, an alternate processing facility may be needed to satisfy immediate operational needs (as in the case of a major natural disaster). In the long term, a new permanent facility must be identified for disaster recovery and equipped to provide for continuation of IS processing services on a regular basis.

Pandemic Planning

Pandemics can be defined as epidemics or outbreaks of infectious diseases in humans that have the ability to spread rapidly over large areas, possibly worldwide, such as flu outbreaks. There are distinct differences between pandemic planning and traditional business continuity planning, and, therefore, the IS auditor should evaluate an organization's preparedness for pandemic outbreaks. Pandemic planning presents unique challenges; unlike natural disasters, technical disasters, malicious acts or terrorist events, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration.

Dealing With Damage to Image, Reputation or Brand

Damaging rumors may rise from many sources. They may or may not be associated with a serious incident or crisis. Whether they are "spontaneous"

or a side effect of a business continuity or disaster recovery problem, their consequences may be devastating. One of the worst consequences of crises is the loss of trust. Effective public relations (PR) activities in an organization may play an important role in helping to contain the damage to the image and ensure that the crisis is not made worse. Certain industries (e.g., banks, health care organizations, airlines, petroleum refineries, chemical, transportation, or nuclear power plants or other organizations with relevant social impact) should have elaborate protocols for dealing with accidents and catastrophes.

A few basic good practices should be considered and applied by an organization experiencing a major incident. Irrespective of the resultant objective consequences of an incident (delay or interruption in service, economic losses, etc.), a negative public opinion or negative rumors can be costly. Reacting appropriately in public (or to the media) during a crisis is not simple. A properly

trained spokesperson should be appointed and prepared

beforehand. Normally, senior legal counsel or a PR officer is the best choice.

No one, irrespective of his/her rank in the organizational hierarchy, except for the spokesperson, should make any public statement.

As part of the preparation, the spokesperson should draft and keep on file a generic announcement with blanks to be filled in with the specific circumstances. This should not be deviated from because of improvisation or time pressure. The announcement should not state the causes of the incident but rather indicate that an investigation has been started and results will be reported. Liability should not be assumed. The system or the process should not be blamed.

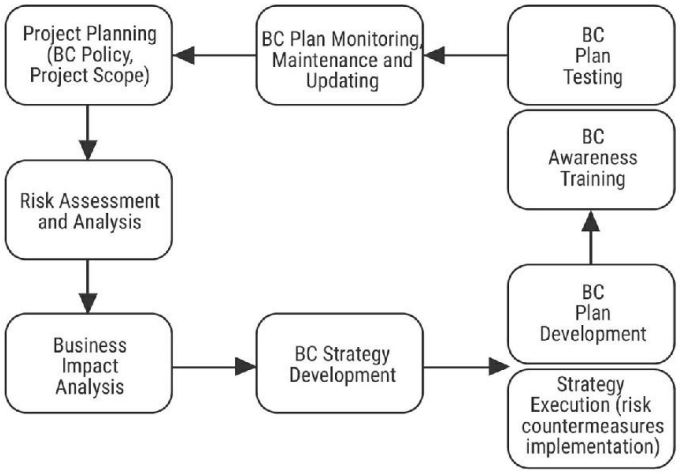
Unanticipated/Unforeseeable Events

Management should consider the possible impacts of unforeseeable (black swan) events on the business of the organization. Black swan events are those events that are a surprise (to the observer), have a major effect and are often inappropriately rationalized with the benefit of hindsight. Black swan events cannot be expected or planned for. Although these events are few and far between, when they occur, they have such a crippling impact on the organization that, based on the criticality of the process or industry or activity, management should start thinking about contingency planning to meet such events. Senior executives who have shared responsibilities being forbidden from traveling together is another example where management is proactive, ensuring that, if a common disaster occurs, the organization would not be left without a senior manager.

4.15.3 BUSINESS CONTINUITY PLANNING PROCESS

The business continuity planning process can be divided into the life cycle phases depicted in **figure 4.30**.

Figure 4.30—Business Continuity Planning Life Cycle



4.15.4 BUSINESS CONTINUITY POLICY

A business continuity policy is a document approved by top management that defines the extent and scope of the business continuity effort (a project or an ongoing program) within the organization. The business continuity policy can be broken into two parts: public and internal. The business continuity policy serves several other purposes:

• Its internal portion is a message to internal stakeholders (i.e., employees, management, board of directors) that the company is undertaking the effort, committing its resources and expecting the rest of the organization to do the same.

• Its public portion is a message to external stakeholders (i.e., shareholders, regulators, authorities, etc.) that the organization is treating its obligations (e.g., service delivery, compliance) seriously.

• It is a statement to the organization, empowering those who are responsible for business continuity.

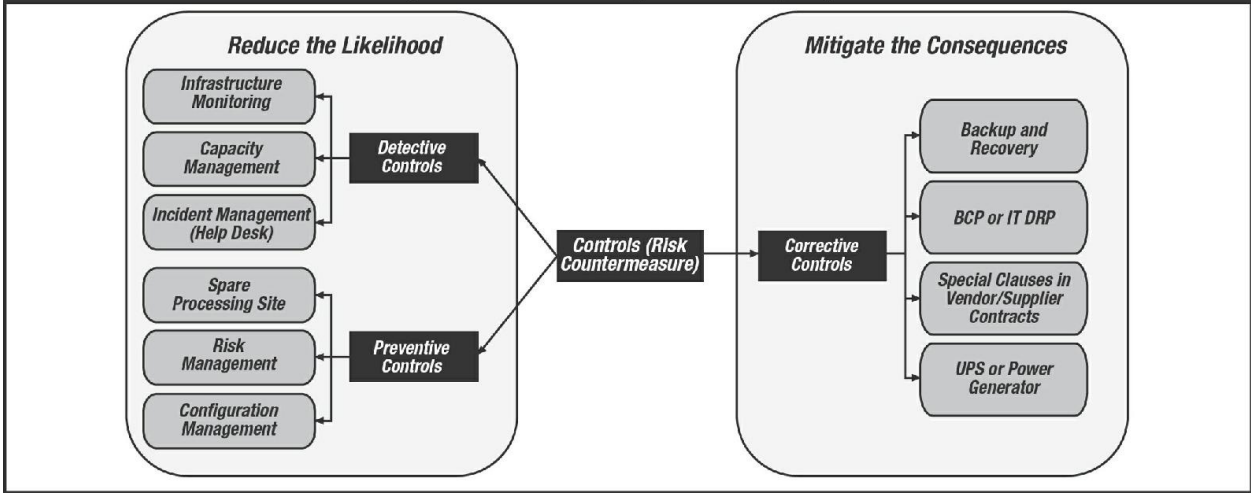
• It may broadly state the general principles on which business continuity will be based.

A business continuity policy should be proactive. The message delivered to the organization must be that all possible controls to detect and prevent disruptions should be used and, if disruption still occurs, to have the controls necessary to

mitigate the consequences. This is later reflected in the IT

business continuity strategy and its execution. There are preventive and

Figure 4.31—Incident and Impact Relationship Diagram



detective controls to reduce the likelihood of a disruption and corrective controls to mitigate the consequences.

The BCP (or IT DRP) is the most critical corrective control. It depends on other controls being effective; in particular, it depends upon incident management and backup and recovery solutions.

Incidents and their impacts can, to some extent, be mitigated through preventive controls. These relationships are depicted in **figure 4.31**.

This requires that the incident management group (help desk) be adequately staffed, supported and trained in crisis management, and that the BCP be well designed, documented, drill tested, funded and audited.

4.15.5 BUSINESS CONTINUITY PLANNING INCIDENT MANAGEMENT

Incidents and crises are dynamic by nature. They evolve, change with time and circumstances, and are often rapid and unforeseeable. Because of this, their management must be dynamic, proactive and well documented. An incident is any unexpected event, even if it causes no significant damage. See section 5.16 Incident Response Management, for more information.

Depending on an estimation of the level of damage to the organization, all types of incidents should be categorized. A classification system could include the following categories: negligible, minor, major and crisis.

Classification can dynamically change while the incident is resolved. These levels can be broadly described as follows:

• **Negligible** incidents are those causing no perceptible or significant damage, such as very brief OS crashes with full information recovery or momentary power outages with UPS backup.

• **Minor** incidents are those that, while not negligible, produce no negative material (of relative importance) or financial impact.

• **Major** incidents cause a negative material impact on business processes and may affect other systems, departments or even outside clients.

• A **crisis** is a major incident that can have serious material (of relative importance) impact on the continued functioning of the business and may also adversely impact other systems or third parties. The severity of the impact depends on the industry and circumstances but is generally directly proportional to the time elapsed from the inception of the incident to incident resolution.

Minor, major and crisis incidents should be documented, classified and revisited until corrected or resolved. This is a dynamic process because a major incident may decrease in extent momentarily and later expand to a crisis incident.

Negligible incidents can be analyzed statistically to identify any systemic or avoidable causes.

Figure 4.32 shows an example of an incident classification system and reaction protocol.

The security officer (SO) or other designated individual should be notified of all relevant incidents as soon as any triggering event occurs. This person should then follow a preestablished escalation protocol (e.g., calling in a spokesperson, alerting top management and involving regulatory agencies) that may be followed by invoking a recovery plan, such as the IT DRP.

Service can be defined as including commitments with clients that can be either

external customers or internal departments. Often, the service delivery is regulated by SLAs which may state the maximum downtime and recovery

Figure 4.32—Incident/Crisis Levels

1 LEVEL		MAIN CRITERION (hours) SERVICE DOWNTIME FORECAST > =	ACTUAL > =	COMPLEMENTARY CRITERIA DATA	PLATFORMS
	7		24		
CRISIS	6	24	12		
	5	12	6	Database loss of integrity	Hacked or Denial of Service Attack
	4	6	4		Viruses, worms. Hardware failure.
MAJOR INC'T	3	4	2		
	2	2	1	Lost transactions	
MINOR INC'T	1	1	0.5		
NEGLIGIBLE	0				

LEVEL		2 ACTIONS		
	7	Follow Business Continuity Plan	Alert SM and eventually Reg. Agencies	
CRISIS	6	Follow Business Continuity Plan	Alert SM and eventually Reg. Agencies	
	5	Prepare for Business Continuity Plan	Alert SM	
	4	Correct/Clean/Restore/Replace	Alert SM	
MAJOR	3	Correct	If confirmed, alert SO	
	2	Correct		
MINOR	1	Correct		
NEGLIGIBLE	0	Log	(Analyze logs regularly)	

SM = Senior Management
SO = Security Officer

estimates. Although not always true, severity is usually driven to a large extent by the estimated downtime.

Other criteria may include the impact on data or platforms and the degree to which the functioning of the organization is adversely impacted. A conservative fail-safe approach would be to assign any nonnegligible incident a starting, provisional severity level 3 (shown in **figure 4.33**). As the incident evolves, this level should be reevaluated regularly by the person or team in charge, often referred to as an incident response or firecall team.

Source: Personas & Técnicas Multimedia SL © 2007. All rights reserved. Used by permission.

4.15.6 DEVELOPMENT OF BUSINESS CONTINUITY

PLANS

Based on the inputs received from the BIA, criticality analysis and recovery strategy selected by management, a detailed BCP and DRP should be developed or reviewed. They should address all the issues included in the business continuity scope that are involved in interruption to business processes,

including recovering from a disaster. The various factors that should be considered while developing/reviewing the plan are:

• Predisaster readiness covering incident response management to address all relevant incidents affecting business processes

• Evacuation procedures

• Procedures for declaring a disaster (rating and escalation procedures)

• Circumstances under which a disaster should be declared. Not all interruptions are disasters, but a small incident if not addressed in a timely or proper manner may lead to a disaster. For example, a virus attack not recognized and contained in time may bring down the entire IT facility.

• The clear identification of the responsibilities in the plan

• The clear identification of the persons responsible for each function in the plan

• The clear identification of contract information

• The step-by-step explanation of the recovery process

• The clear identification of the various resources required for recovery and continued operation of the organization

The plan should be documented and written in simple language,

understandable to all.

It is common to identify teams of personnel who are made responsible for specific tasks in case of disasters. Some important teams should be formed, and their responsibilities are explained in the next section. Copies of the plan should be maintained offsite. The plan must be structured so that its parts can easily be handled by different teams.

4.15.7 OTHER ISSUES IN PLAN DEVELOPMENT

The personnel who must react to the interruption/disaster are those responsible for the most critical resources. Therefore, management and user involvement is

vital to the success of the execution of the BCP. User management involvement is essential to the identification of critical systems, their associated critical recovery times and the specification of needed resources. The three major divisions that require involvement in the formulation of the BCP are support services (who detect the first signs of incident/disaster), business operations (who may suffer from the incident) and information processing support (who are going to run the recovery).

Because the underlying purpose of BCP is the recovery and resumption of business operations, it is essential to consider the entire organization, not just

IS processing services, when developing the plan. Where a uniform BCP

does not exist for the entire organization, the plan for IS processing should be extended to include planning for all divisions and units that depend on IS

processing functions.

When formulating the plan, the following items should also be included:

• A list of the staff, with redundant contact information (backups for each contact), required to maintain critical business functions in the short, medium and long term.

• The configuration of building facilities, desks, chairs, telephones, etc., required to maintain critical business functions in the short, medium and long term

• The resources required to resume/continue operations (not necessarily IT or even technology resources)

4.15.8 COMPONENTS OF A BUSINESS CONTINUITY

PLAN

Depending on the size and/or requirements of an organization, a BCP may consist of more than one plan document. A BCP should include:

• Continuity of operations plan

• DRP

• Business resumption plan

A BCP may also include:

• Continuity of support plan/IT contingency plan

• Crisis communications plan

• Incident response plan

• Transportation plan

• Occupant emergency plan

• Evacuation and emergency relocation plan

One example of the components of a BCP, suggested by *NIST Special Publication 800-34 Revision 1: Contingency Planning Guide for Federal Information Systems*, is shown in **figure 4.33**.

For the planning, implementation and evaluation phase of the BCP, the

Figure 4.33—Components of a Business Continuity Plan

Plan	Purpose	Scope	Plan Relationship
Business continuity plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption.	Address mission/business processes at a lower or expanded level from COOP MEFs.	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-MEFs.
Continuity of operations (COOP) plan	Provides procedures and guidance to sustain an organization's MEFs at an alternate site for up to 30 days; mandated by federal directives.	Addresses MEFs at a facility; information systems are addressed based only on their support of the mission essential functions.	MEF focused plan that may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate.

Crisis communications Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system-focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components as defined in the National Infrastructure Protection Plan.	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets.
Cyberincident response plan	Provides procedures for mitigating and correcting a cyberattack, such as a virus, worm, or Trojan horse.	Address mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system-focused plan that may activate an ISCP or DRP depending on the extent of the attack.
Disaster recovery plan (DRP)	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long-term effects.	Information system-focused plan that activates one or more ISCPs for recovery of individual systems.
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system.	Addresses single information system recovery at the current or, if appropriate alternate location.	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
Occupant emergency plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

following should be agreed on:

Source: National Institute of Standards and Technology, *NIST Special Publication 800-34 Revision 1: Contingency Planning Guide for Federal Information Systems*, USA, 2010. Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

• The policies that will govern all of the continuity and recovery efforts

• The goals/requirements/products for each phase

• Alternate facilities to perform tasks and operations

• Critical information resources to deploy (e.g., data and systems)

• Persons responsible for completion

• Available resources to aid in deployment (including human)

• The scheduling of activities with priorities established

Most BCPs are created as procedures that accommodate recovery of

information systems (i.e., data storage, servers, etc.), user workstations, other selected equipment (card readers, barcode scanners, printers, etc.) and the network (channels, equipment). Copies of the plan should be kept offsite—at the recovery facility, at the media storage facility and possibly at the homes of key decision-making personnel. More and more frequently, an

organization places the electronic version of the plan on a mirrored website.

Key Decision-making Personnel

The plan should contain a telephone list or call tree (i.e., a notification directory of key decision-making IT and end-user personnel who are required to initiate and carry out recovery efforts). This is usually a telephone directory of people who should be notified if an incident/disaster or catastrophe occurs, and it often can be automated. Points to remember when preparing the list are:

• In the event of a widespread disaster or a fire/explosion during normal business hours that heavily damages the organization's offices, many team leaders may not be available

• The call tree should be highly redundant, maintained on hard copy and possibly on an intranet, and updated on a regular basis.

This directory should contain the following information:

• A prioritized list of contacts (i.e., who gets called first?)

• Primary and emergency telephone numbers and addresses for each critical contact person. These usually will be key team leaders responsible for contacting the members of their team.

• Phone numbers and addresses for representatives of equipment and software vendors

• Phone numbers of contacts within companies that have been designated to provide supplies and equipment or services

• Phone numbers of contact persons at recovery facilities, including hot-site representatives and predefined network communications rerouting services

• Phone numbers of contact persons at offsite media storage facilities and the contact persons within the company who are authorized to retrieve media from the offsite facility

• Phone numbers of insurance company agents

• Phone numbers of contacts at contract personnel services

• Phone numbers and contacts of legal/regulatory/governmental agencies, if required

• A procedure to ascertain how many people were reached while using the call tree

Backup of Required Supplies

The plan should have provisions for all supplies necessary for the continuation of normal business activities in the recovery effort. This includes detailed, up-to-date hard copy procedures that can be followed easily by staff and contract personnel who are unfamiliar with the standard and recovery operations. Also, a supply of special forms, such as check stock, invoice forms and order forms, should be secured at an offsite location.

If the data entry function depends on certain hardware devices and/or software programs, these programs and equipment should be provided at the hot site. The same applies to cryptographic equipment, including electronic keys (e.g., RSA tokens and USB keys).

Insurance

The plan should contain key information about the organization’s insurance.

The IT processing insurance policy is usually a multi-peril policy designed to provide various types of IT coverage. It should be constructed in modules so it can be adapted to the insured’s particular IT environment.

Note: Specifics on insurance policies are not tested on the CISA exam because they differ from country to country. The test covers what should be included in policies and third-party agreements but would not test the specific types of coverage.

Specific types of coverage available are:

• **IT equipment and facilities**—Provides coverage for physical damage to the IPF and owned equipment. (Insurance of leased equipment should be obtained when the lessee is responsible for hazard coverage.) The IS

auditor is cautioned to review these policies because many policies obligate insurance vendors to replace nonrestorable equipment only with “like kind

and quality,” not necessarily with new equipment by the same vendor as the damaged equipment.

• **Media (software) reconstruction**—Covers damage to IT media that is the property of the insured and for which the insured may be liable. Insurance is available for on-premises, off-premises or in-transit situations and covers the actual reproduction cost of the property. Considerations in determining the amount of coverage needed are programming costs to reproduce the media damaged; backup expenses; and physical replacement of media devices, such as tapes, cartridges and disks.

• **Extra expense**—Designed to cover the extra costs of continuing operations following damage or destruction at the IPF. The amount of extra-expense insurance needed is based on the availability and cost of backup facilities and operations. Extra expense can also cover the loss of net profits caused by computer media damage. This provides reimbursement for monetary losses resulting from suspension of operations due to the physical loss of equipment or media. An example of a situation requiring this type of coverage is if the information processing facilities were on the sixth floor and the first five floors were burned out. In this case, operations would be interrupted even though the IPF remained unaffected.

• **Business interruption**—Covers the loss of profit due to the disruption of the activity of the company caused by any malfunction of the IT

organization

• **Valuable papers and records**—Covers the actual cash value of papers and records (not defined as media) on the insured’s premises against direct physical loss or damage

• **Errors and omissions**—Provides legal liability protection if the professional practitioner commits an act, error or omission that results in financial loss to a client. This insurance was originally designed for service bureaus but it is now available from several insurance companies for protecting systems analysts, software designers, programmers, consultants and other IS personnel.

• **Fidelity coverage**—Usually takes the form of bankers blanket bonds, excess fidelity insurance and commercial blanket bonds and covers loss from dishonest or fraudulent acts by employees. This type of coverage is prevalent in financial institutions operating their own IPF.

• **Media transportation**—Provides coverage for potential loss or damage to

media in transit to off-premises IPFs. Transit coverage wording in the policy usually specifies that all documents must be filmed or otherwise copied. When the policy does not state specifically that data be filmed prior to being transported and the work is not filmed, management should obtain from the insurance carrier a letter that specifically describes the carrier's position and coverage if data are destroyed.

Several key points are important to remember about insurance. Most insurance covers only financial losses based on the historical level of performance and not on the existing level of performance. The IS auditor will also be concerned with ensuring that the valuation of insured items, such as technical equipment and infrastructure and data, is appropriate and up to date.

Also, insurance does not compensate for loss of image/goodwill.

4.15.9 PLAN TESTING

Most business continuity tests fall short of a full-scale test of all operational portions of the organization, if they are in fact tested at all. This should not preclude performing full or partial testing because one of the purposes of the business continuity test is to determine how well the plan works or which portions of the plan need improvement.

The test should be scheduled during a time that will minimize disruptions to normal operations. Weekends are generally a good time to conduct tests. It is important that the key recovery team members be involved in the test process and allotted the necessary time to put their full effort into it. The test should

address all critical components and simulate actual primetime processing conditions, even if the test is conducted in off hours.

Specifications

The test should strive to accomplish the following tasks:

• Verify the completeness and precision of the BCP.

• Evaluate the performance of the personnel involved in the exercise.

• Appraise the training and awareness of employees who are not members of a business continuity team.

• Evaluate the coordination among the business continuity team and external vendors and suppliers.

• Measure the ability and capacity of the backup site to perform prescribed processing.

• Assess the vital records retrieval capability.

• Evaluate the state and quantity of equipment and supplies that have been relocated to the recovery site.

• Measure the overall performance of operational and IT processing activities related to maintaining the business entity.

Note: Assessing the results and the value of the BCP and the DRP tests is an important part of the IS auditor's responsibility.

Test Execution

To perform testing, each of the following test phases should be completed:

• **Pretest**—The set of actions necessary to set the stage for the actual test.

This ranges from placing tables in the proper operations recovery area to transporting and installing backup telephone equipment. These activities are outside the realm of those that would take place in the case of a real emergency, in which there is no forewarning of the event and, therefore, no time to take

preparatory actions.

• **Test**—This is the real action of the business continuity test. Actual operational activities are executed to test the specific objectives of the BCP. Data entry, telephone calls, information systems processing, handling orders, and movement of personnel, equipment and suppliers should take place. Evaluators review staff members as they perform the designated tasks. This is the actual test of preparedness to respond to an emergency.

• **Posttest**—The cleanup of group activities. This phase comprises such assignments as returning all resources to their proper place, disconnecting equipment, returning personnel, and deleting all company data from third-party systems. The posttest cleanup also includes formally evaluating the plan and implementing indicated improvements.

In addition, the following types of tests may be performed:

• **Desk-based evaluation/paper test**—A paper walk-through of the plan, involving major players in the plan's execution who reason out what might happen in a particular type of service disruption. They may walk through

the entire plan or just a portion. The paper test usually precedes the preparedness test.

• **Preparedness test**—Usually a localized version of a full test, wherein actual resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about how good the plan is. It also provides a means to improve the plan in increments.

• **Full operational test**—This is one step away from an actual service disruption. The organization should have tested the plan well on paper and locally before endeavoring to completely shut down operations. For purposes of the BCP testing, this is the disaster.

Documentation of Results

During every phase of the test, detailed documentation of observations, problems and resolutions should be maintained.

Each team should have a diary form, with specific steps and information to be recorded, which can be used as documentation. This documentation serves as important historical information that can facilitate actual recovery during a real disaster.

Additionally, the insurance company or the local authorities may ask for it.

The documentation also aids in performing detailed analysis of both the strengths and weaknesses of the plan.

Results Analysis

It is important to have ways to measure the success of the plan and test against the stated objectives. Therefore, results must be quantitatively gauged as opposed to an evaluation that is based only on observation.

Specific measurements vary depending on the test and the organization; however, the following general measurements usually apply:

• Time—Elapsed time for completion of prescribed tasks, delivery of equipment, assembly of personnel and arrival at a predetermined site

• Amount—Amount of work performed at the backup site by clerical personnel and information systems processing operations

• Count—The number of vital records successfully carried to the backup site versus the required number and the number of supplies and equipment requested versus actually received. Also, the number of critical systems successfully recovered can be measured with the number of transactions processed.

• Accuracy—Accuracy of the data entry at the recovery site versus normal accuracy (as a percentage). Also, the accuracy of actual processing cycles can be determined by comparing output results with those for the same period processed under normal conditions.

Plan Maintenance

Plans and strategies for business continuity should be reviewed and updated on a scheduled basis to reflect continuing recognition of changing requirements or extraordinarily (unscheduled revisions) when there is an important change

affecting the plans and strategies. The following factors, and others, may impact business continuity requirements and the need for the plan to be updated:

• A strategy that is appropriate at one point in time may not be adequate as the needs of the organization change (business processes, new departments, changes in key personnel).

• New resources/applications may be developed or acquired.

• Changes in business strategy may alter the significance of critical applications or deem additional applications as critical.

• Changes in the software or hardware environment may make current provisions obsolete or inappropriate.

• New events or a change in the likelihood of events may cause disruption.

• Changes are made to key personnel or their contact details.

An important step in maintaining a BCP is to update and test it whenever relevant changes take place within the organization. It is also desirable to include BCP as part of the SDLC process.

The responsibility for maintaining the BCP often falls on the BCP

coordinator. Specific plan maintenance responsibilities include:

• Develop a schedule for periodic review and maintenance of the plan advising all personnel of their roles and the deadline for receiving revisions

and comments.

• Call for unscheduled revisions when significant changes have occurred.

• Review revisions and comments and updating the plan within a certain number days (e.g., 30 days, 2 weeks) of the review date.

• Arrange and coordinate scheduled and unscheduled tests of the BCP to evaluate its adequacy.

• Participate in the scheduled plan tests, which should be performed at least once

per year on specific dates. For scheduled and unscheduled tests, the coordinator will write evaluations and integrate changes to resolve unsuccessful test results into the BCP within a certain number of days (e.g., 30 days, 2 weeks).

• Develop a schedule for training recovery personnel in emergency and recovery procedures as set forth in the BCP. Training dates should be scheduled within 30 days of each plan revision and scheduled plan test.

• Maintain records of BCP maintenance activities—testing, training and reviews.

• Periodically update, at least quarterly (shorter periods are recommended), the notification directory of all personnel changes including phone numbers, responsibilities or status within the company.

A software tool for administering continuity and recovery plans may be useful to track and follow-up on maintenance tasks.

Business Continuity Management Good Practices

The need to continually and periodically revisit and improve on the business continuity program is critical to the development of successful and robust recovery strategy for an organization, irrespective of whether the organization is at the initial stage of developing a BCP. In an effort to enhance business continuity management capabilities (and to comply with regulatory guidelines), some organizations have started adopting good practices from industry-independent and industry-specific entities and regulatory agencies.

Some of the following entities or practices/regulations/standards are:

• Business Continuity Institute (BCI)—Provides good practices for business continuity management

• Disaster Recovery Institute International (DRII)—Provides professional

practices for business continuity professionals

• US Federal Emergency Management Association (FEMA)—Provides

business and industry guidance for emergency management

• ISACA—The COBIT framework provides guidance on IT controls that are relevant to the business.

• US National Institute of Standards and Technology (NIST)

• US Federal Financial Institutions Examination Council (FFIEC)

• US Health and Human Services (HHS)—The Health Insurance Portability and Accountability Act (HIPAA) describes the requirements for managing health information.

• *ISO 22301:2012: Societal security—Business continuity management systems —Requirements*

Note: The CISA candidate will not be tested on specific

practices/regulations/standards.

4.15.10 SUMMARY OF BUSINESS CONTINUITY

To ensure continuous service, a BCP should be written to minimize the impact of disruptions. This plan should be based on the long-range IT plan and should support and be aligned with the overall business continuity strategy The process of developing and maintaining an appropriate DRP/BCP

follows:

• Conduct a risk assessment.

• Identify and prioritize the systems and other resources required to support critical business processes in the event of a disruption.

• Identify and prioritize threats and vulnerabilities.

• Prepare BIA of the effect of the loss of critical business processes and their supporting components.

• Choose appropriate controls and measures for recovering IT components to support the critical business processes.

• Develop the detailed plan for recovering IS facilities (DRP).

• Develop a detailed plan for the critical business functions to continue to operate at an acceptable level (BCP).

• Test the plans.

• Maintain the plans as the business changes and systems develop.

4.15.11 AUDITING BUSINESS CONTINUITY

The IS auditor’s tasks include:

• Understand and evaluate business continuity strategy and its connection to business objectives.

• Review the BIA findings to ensure that they reflect current business priorities and current controls.

• Evaluate the BCPs to determine their adequacy and currency, by reviewing the plans and comparing them to appropriate standards and/or government regulations including the RTO, RPO, etc., defined by the BIA.

• Verify that the BCPs are effective, by reviewing the results from previous tests performed by IT and end-user personnel.

• Evaluate cloud-based mechanisms.

• Evaluate offsite storage to ensure its adequacy, by inspecting the facility and reviewing its contents and security and environmental controls.

• Verify the arrangements for transporting backup media to ensure that they meet the appropriate security requirements.

• Evaluate the ability of personnel to respond effectively in emergency situations, by reviewing emergency procedures, employee training and results of their tests and drills.

• Ensure that the process of maintaining plans is in place and effective and covers both periodic and unscheduled revisions.

• Evaluate whether the business continuity manuals and procedures are written in

a simple and easy to understand manner. This can be achieved through interviews and determining whether all the stakeholders

understand their roles and responsibilities with respect to business continuity strategies.

Reviewing the Business Continuity Plan

When reviewing the plan, IS auditors should verify that basic elements of a well-developed plan are evident. The following paragraphs list the audit procedures to address the basic BCP elements.

Review the Document

• Obtain a copy of the current business continuity policy and strategy.

• Obtain a current copy of the BCP or manual.

• Obtain a copy of the most recent BIA findings and identify the RTO, RPO

and other key strategic directives.

• Sample the distributed copies of the manual and verify that they are current.

• Verify whether the BCP supports the overall business continuity strategy.

• Evaluate the effectiveness of the documented procedures for the invocation of the BCP execution.

• Evaluate the procedure for updating the manual. Are updates applied and distributed in a timely manner? Are specific responsibilities documented for maintenance of the manual?

Review the Applications Covered by the Plan

• Review the identification, priorities and planned support of critical applications, both server-based and workstation-based applications.

• Determine whether all applications have been reviewed for their level of tolerance in the event of a disaster.

• Determine whether all critical applications (including PC applications) have been identified.

• Determine whether the secondary site has the correct versions of all system software. Verify that all of the software is compatible; otherwise, the system will not be able to process production data during recovery.

Review the Business Continuity Teams

• Obtain a member list for each recovery/continuity/response team.

• Obtain a copy of agreements relating to use of backup facilities.

• Review the list of business continuity personnel, emergency hot-site contacts, emergency vendor contacts, etc., for appropriateness and completeness.

• Call a sample of the people indicated and verify that their phone numbers and addresses are correct, as indicated, and that they possess a current copy of the business continuity manual.

• Interview them for an understanding of their assigned responsibilities in case of interruption/disaster situation.

Plan Testing

• Evaluate the procedures for documenting the tests.

• Review the backup procedures followed for each area covered by the DRP.

• Determine whether the backup and recovery procedures are being followed.

In addition to the previous steps, the IS auditor should:

• Evaluate whether all written emergency procedures are complete, appropriate, accurate, current and easy to understand.

• Identify whether the transactions reentered in the system through recovery process need to be separately identified from the normal transactions.

• Determine whether all recovery/continuity/response teams have written procedures to follow in the event of a disaster.

• Determine whether a suitable procedure exists for updating the written emergency procedures.

• Determine whether user recovery procedures are documented.

• Determine whether the plan adequately addresses movement to the recovery site.

• Determine whether the plan adequately addresses recovering from the recovery site.

• Determine whether items necessary for the reconstruction of the information processing facility are stored offsite, such as blueprints, hardware inventory and wiring diagrams.

Questions to consider include:

• Who is responsible for administration or coordination of the plan?

• Is the plan administrator/coordinator responsible for keeping the plan up to date?

• Where is the DRP stored?

• What critical systems are covered by the plan?

• What systems are not covered by the plan? Why not?

• What equipment is not covered by the plan? Why not?

• Does the plan operate under any assumptions? What are they?

• Does the plan identify rendezvous points for the disaster management committee or emergency management team to meet and decide if business continuity should be initiated?

• Are the documented procedures adequate for successful recovery?

• Does the plan address disasters of varying degrees?

• Are telecommunication’s backups (both data and voice line backups) addressed

in the plan?

• Where is the backup facility site?

• Does the plan address relocation to a new information processing facility if the original center cannot be restored?

• Does the plan include procedures for merging master file data, automated tape management system data, etc., into predisaster files?

• Does the plan address loading data processed manually into an automated system?

• Are there formal procedures that specify backup procedures and responsibilities?

• What training has been given to personnel in using backup equipment and established procedures?

• Are the restoration procedures documented?

• Are regular and systematic backups of required sensitive and/or crucial applications and data files, being taken?

• Who determines the methods and frequency of data backup for critical information stored?

• What type of media is being used for backups?

• Is offsite storage used to maintain backups of critical information required for processing either onsite or offsite operations?

• Is there adequate documentation to perform a recovery in case of disaster or loss of data?

• Is there a schedule for testing and training on the plan?

• Are the requirements for normal operations and disasters defined in the relevant SLAs with regard to how the service will operate?

Evaluation of Prior Test Results

The BCP coordinator should maintain historical documentation of the results of prior business continuity tests. The IS auditor should review these results and determine whether actions requiring correction have been incorporated into the plan. Also, the IS auditor should evaluate BCP/DRP prior tests for thoroughness and accuracy in accomplishing their objectives. Test results should be reviewed to determine whether the appropriate results were

achieved and to determine problem trends and appropriate resolutions of problems.

Evaluation of Offsite Storage

The offsite storage facility should be evaluated to ensure the presence, synchronization and currency of critical media and documentation. This includes data files, applications software, applications documentation, systems software, systems documentation, operations documentation, necessary supplies, special forms and a copy of the BCP. To verify the conditions mentioned above, the IS auditor should perform a detailed inventory review. This inventory includes testing for correct dataset names, volume serial numbers, accounting periods and bin locations of media. The IS auditor should also review the documentation, compare it for currency with production documentation, evaluate the availability of the facility and ensure it conforms with management’s requirements.

The IS auditor should also review the method of transporting backup data to and from the offsite storage facility to ensure it does not represent a weakness in the information security management system.

Evaluation of Security at the Offsite Facility

The security of the offsite facility should be evaluated to ensure that it has the proper physical and environmental access controls. These controls include:

• Ability to limit access to only authorized users of the facility

• Raised flooring

• Humidity controls

• Temperature controls

• Specialized circuitry

• Uninterruptible power supply

• Water detection devices

• Smoke detectors

• Appropriate fire extinguishing system.

The IS auditor should examine the equipment for current inspection and calibration tags. This review should also consider the security requirements of media transportation.

Interviewing Key Personnel

The IS auditor should interview key personnel required for the successful recovery of business operations. All key personnel should understand their assigned responsibilities and up-to-date detailed documentation describing their tasks.

Reviewing the Alternative Processing Contract

The IS auditor should obtain a copy of the contract with the vendor of the alternative processing facility. The vendor's references should be checked to ensure reliability, and all vendor promises should be verified in writing. The contract should be reviewed against the following guidelines:

• Ensure that the contract is written clearly and is understandable.

• Ensure there was a legal review for required terms and the condition to meet all applicable laws and regulations.

• Reexamine and confirm the organization's agreement with the rules that apply to sites shared with other subscribers.

• Ensure that insurance coverage ties in with and covers all (or most) expenses of the disaster.

• Ensure that tests can be performed at the hot site at regular intervals.

• Review and evaluate communications requirements for the backup site.

• Ensure that enforceable source code escrow is reviewed by a lawyer specializing in such contracts.

• Determine the limitation recourse tolerance in the event of a breached agreement.

Reviewing Insurance Coverage

It is essential that insurance coverage reflects the actual cost of recovery.

Taking into consideration the insurance premium (cost), the coverage for media damage, business interruption, equipment replacement and business continuity processing should be reviewed for adequacy. The specific areas of risk should be found within the BIA, customer contracts and SLAs along with regulatory impacts due to a break in business operations.

Note: The CISA candidate should know what critical provisions need to be included within insurance policies to safeguard the organization

4.16 DISASTER RECOVERY PLANS

Disaster recovery planning, in support of business operations/provisioning IT

service, is an element of an internal control system established to manage availability and restore critical processes/IT services in the event of interruption. The purpose of this continuous planning process is to ensure that cost-effective controls are in place to prevent possible IT disruptions and to recover the IT capacity of the organization in the event of a disruption. The importance of the availability of individual applications/IT services depends on the importance of the business processes that they support. The importance and urgency of these business processes and corresponding IT

services and applications can be defined through performing a BIA and assigning RPOs and RTOs. The availability of business data and the ability to process and handle them are vital to the sustainable development and/or survival of any organization. Planning for disasters is, therefore, an important part of the risk management and business continuity planning processes.

Disaster recovery planning is a continuous process. After the criticality of business processes and supporting IT services, systems and data are defined, they are periodically reviewed and revisited. There are at least the following two important outcomes of disaster recovery planning:

• Changes in IT infrastructure (servers, networks, data storage systems, etc.), changes in supporting processes (increasing the maturity), procedures and organizational structure (new headcount or new roles). These changes are combined into programs spanning three to five years, often called IT DR

strategies.

• DRPs developed as part of this process that direct the response to incidents ranging from simple emergencies to full-blown disasters. The plans range from departmental-level, simple procedures down to modular, multitiered plans that cover multiple locations and multiple lines of business.

The ultimate goal of the disaster recovery planning process is to respond to incidents that may impact people and the ability of operations to deliver goods and services to the marketplace and to comply with regulatory requirements.

Disaster recovery planning may be subject to various compliance requirements depending upon geographic location, nature of business, and the legal and regulatory framework. Organizations engage third parties to perform the activities on their behalf, and these third parties are still subject to compliance. Most compliance requirements will focus on assuring continuity of service; however, human safety is the most essential aspect. For example, in case of fire, safe evacuation comes first; restoring service is a secondary activity.

This section focuses on the key activities that an organization must perform to proactively plan for, and manage, the consequences of a disaster.

4.16.1 RECOVERY POINT OBJECTIVE AND RECOVERY

TIME OBJECTIVE

The RPO is determined based on the acceptable data loss in case of disruption of operations. It indicates the earliest point in time in which it is acceptable to recover the data. For example, if the process can afford to lose the data up to four hours before disaster, then the latest backup available should be up to four

hours before disaster or interruption and the transactions that occurred during the RPO period and interruption need to be entered after recovery (known as catch-up data).

It is almost impossible to recover the data completely. Even after entering incremental data, some data are still lost and are referred to as orphan data.

The RPO directly affects the technology used to back up and recover data (see **figure 4.34**).

The RTO is determined based on the acceptable downtime in case of a disruption of operations. It indicates the earliest point in time at which the business operations (and supporting IT systems) must resume after disaster.

Figure 4.34 shows the relationship between the RTO and RPO and gives examples of technologies used to meet the RPOs and RTOs.

Both of these concepts are based on time parameters. The nearer the time requirements are to the center (0-1 hours), the higher the cost of the recovery strategies. If the RPO is in minutes (lowest possible acceptable data loss),

then data mirroring or real-time replication should be implemented as the recovery strategy. If the RTO is in minutes (lowest acceptable time down), then a hot site, dedicated spare servers (and other equipment) and clustering must be used.

Disaster tolerance is the time gap within which the business can accept the unavailability of IT critical service; therefore, the lower the RTO, the lower the disaster tolerance.

RTO affects the technology used to make applications/IT systems available—

what to use for recovery (e.g., warm site, hot site, clusters). RPO usually affects data protection solutions (backup and recovery, synchronous or asynchronous data replication).

Note: The CISA candidate should be familiar with which recovery strategies would be best with different RTO and RPO parameters.

In addition to RTO and RPO, there are some additional parameters that are

important in defining the recovery strategies. These include:

• **Interruption window**—The maximum period of time the organization can wait from the point of failure to the critical services/applications restoration. After this time, the progressive losses caused by the interruption are unaffordable.

• **Service delivery objective (SDO)**—Level of services to be reached during the alternate process mode until the normal situation is restored. This is directly related to the business needs.

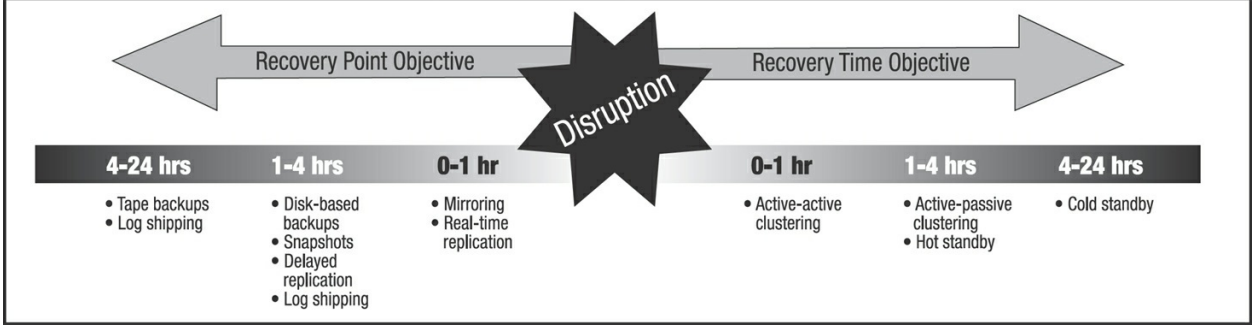
• **Maximum tolerable outages (MTOs)**—Maximum time the organization can support processing in alternate mode. After this point, different problems may arise, especially if the alternate SDO is lower than the usual SDO, and the information pending to be updated can become

unmanageable.

4.16.2 RECOVERY STRATEGIES

A recovery strategy identifies the best way to recover a system (one or many) in case of interruption, including disaster, and provides guidance based on

Figure 4.34—Relationship Between RTO and RPO



which detailed recovery procedures can be developed. Different strategies should be developed, and all alternatives should be presented to senior management. Senior management should select the most appropriate strategies from the alternatives provided and accept the inherent residual risk.

The selected strategies should be used to further develop the detailed BCP.

The selection of a recovery strategy depends on:

• The criticality of the business process and the applications supporting the processes

• Cost

• Time required to recover

• Security

There are various strategies for recovering critical information resources. The appropriate strategy is the one with a cost for an acceptable recovery time that is also reasonable compared to the impact and likelihood of occurrence as determined in the BIA. The cost of recovery is the cost of preparing for possible disruptions (e.g., the fixed costs of purchasing, maintaining and regularly testing redundant computers, and maintaining alternate network routing), and the variable costs of putting these into use in the event of a disruption. The latter costs can often be insured against, but the former generally cannot. However, the premiums for disaster insurance usually will be lower if there is a suitable plan.

Generally, each IT platform that runs an application supporting a critical business function will need a recovery strategy. There are many alternative

strategies. The most appropriate alternative, in terms of cost to recover and impact cost, should be selected based on the relative risk level identified in the business impact analysis. Recovery strategies based on the risk level identified for recovery include developing:

• Hot sites

• Warm sites

• Cold sites

• Duplicate information processing facilities

• Mobile sites

• Reciprocal arrangements with other organizations

4.16.3 RECOVERY ALTERNATIVES

When the normal production facilities become unavailable, the business may use alternate facilities to sustain critical processing until the primary facilities can be restored. **Figure 4.35** lists the most common recovery alternatives.

Alternatives that provide the fastest recovery time require the most dedicated resources on an ongoing basis, and thus incur the greatest cost to the company. By comparing the business costs associated with the interruption of critical processes (developed in the BIA) to the cost of the various alternative processing options, management will establish an optimal RTO and select an appropriate recovery alternative.

The alternate site should be selected with consideration that it will be located beyond the geographic area affected by any disruptive events considered in the plan. The impact and nature of the disruptive events should be considered in determining an adequate separation from the primary site rather than specifying a particular distance of separation.

Regardless of which type of alternative processing is used, the plan needs to include the provision to establish network communication to the alternate site. The plan should provide for redundant solutions to ensure that communications can be established to the alternate site following interruption of normal processing by any anticipated cause.

Figure 4.35—Recovery Alternatives

Cold sites are facilities with the space and basic infrastructure adequate to support resumption of operations, but lacking any IT or communications equipment, programs, data or office support. A plan that specifies that a cold site will be utilized must also include provision to acquire and install the requisite hardware, software and office equipment to support the critical applications when the plan is activated. To use a sports analogy, a cold site is like having a substitute on the bench, ready to be called into the game.

Mobile sites are packaged, modular processing facilities mounted on transportable vehicles and kept ready to be delivered and set up at a location that may be specified upon activation. A plan to utilize mobile processing must specify the site locations that may be used. The plan must provide right-of-access to the selected site by the vendor and the company. The plan must also

provide for any required ancillary infrastructure necessary to support the site such as access roads, water, waste disposal, power and communications.

Warm sites are complete infrastructures but are partially configured in terms of IT, usually with network connections and essential peripheral equipment such as disk drives, tape drives and controllers. The equipment may be less capable than the normal production equipment yet still be adequate to sustain critical applications on an interim basis. Typically, employees would be transferred to the warm site, and current versions of programs and data would need to be loaded before operations could resume at the warm site. Using the sports analogy, a warm site is a substitute warming up, getting ready to enter the game.

Hot sites are facilities with space and basic infrastructure and all of the IT and communications equipment required to support the critical applications, along with office furniture and equipment for use by the staff. Hot sites usually maintain installed versions of the programs required to support critical applications. Data may also be duplicated to the hot site in real or near real time. If this is not the case the most recent backup copies of data may need to be loaded before critical applications could be resumed. Although hot sites may have a small staff assigned, employees are usually transferred to the hot site from the primary site to support operations upon activation. Using the sports analogy, a hot site is a substitute on the sideline waiting to enter the game.

Mirrored sites are fully redundant sites with real-time data replication from the production site.

They are fully equipped and staffed, and can assume critical processing with no interruption perceived by the users.

Reciprocal agreements are agreements between separate, but similar, companies to temporarily share their IT facilities in the event that one company loses processing capability. Reciprocal agreements are not considered a viable option due to the constraining burden of maintaining hardware and software compatibility between the companies, the complications of maintaining security and privacy compliance during shared operations, and the difficulty of enforcing the agreements should a disagreement arise at the time the plan is activated.

Reciprocal agreements with other organizations, although a less frequently used method, are agreements between two or more organizations with unique

equipment or applications. Under the typical agreement, participants promise to provide assistance to each other when an emergency arises.

The alternate processing facility can be provided by a third-party vendor or by the company using its own resources. When the facility is owned by the company, priority and conflicts can be prevented or quickly resolved by

senior management. When the facility is provided by a third party, the company needs to have clearly stated contracts that ensure that the company will get access to the resources it needs without delay following a disaster.

Consideration must be given to the likelihood that at the same time that the company needs to utilize the alternate processing facility, other companies in the area may also be trying to restore critical processing.

Contractual Provisions

Contractual provisions for the use of third-party sites should cover the following:

• **Configurations**—Are the hardware and software configurations for the facility adequate to meet company needs? Is there provision to update the configurations and conduct tests to ensure that the configurations remain adequate over time?

• **Disaster**—Is the definition of disaster broad enough to meet anticipated needs?

• **Access**—Is use of the facility exclusive or does the customer have to share the available space if multiple customers simultaneously declare a disaster?

Does the company have guaranteed assurance that they will have adequate access to the site and the resources following a disaster? Does the agreement satisfactorily specify how access conflicts will be resolved?

• **Priority**—Does the agreement provide the company with satisfactory priority following a disaster? Does the agreement preclude the sharing of the needed resources with governmental entities that might preempt the company following a disaster?

• **Availability**—Will the facility be available to the company without delay when needed?

• **Speed of availability**—How soon after a disaster will facilities be available?

• **Subscribers per site**—Does the agreement limit the number of subscribers per site?

• **Subscribers per area**—Does the agreement limit the number of subscribers in a building or area?

• **Preference**—Who gets preference if there are common or regional disasters? Is there backup for the backup facilities? Is use of the facility exclusive or does the customer have to share the available space if multiple

customers simultaneously declare a disaster? Does the vendor have more than one facility available for subscriber use?

• **Insurance**—Is there adequate insurance coverage for company employees at the backup site? Will existing insurance reimburse those fees?

• **Usage period**—How long is the facility available for use? Is this period adequate? What technical support will the site operator provide? Is this adequate?

• **Communications**—Are the communications adequate? Are the communication connections to the backup site sufficient to permit unlimited communication with the alternate site if needed?

• **Warranties**—What warranties will the vendor make regarding availability of the site and the adequacy of the facilities? Are there liability limitations (there usually are) and is the company willing to live with them?

• **Audit**—Is there a right-to-audit clause permitting an audit of the site to evaluate the logical, physical and environmental security?

• **Testing**—What testing rights are included in the contract? Check with the insurance company to determine any reduction of premiums that may be forthcoming due to the backup site availability.

• **Reliability**—Can the vendor attest to the reliability of the site(s) being offered? Ideally, the vendor should have an UPS, limited subscribers, sound technical management, and guarantees of computer hardware and software compatibility.

• **Security**—Can the site be adequately secured by the company to comply with the company's security policy?

Procuring Alternative Hardware

Companies planning to use a cold or warm site will need to include in their plan provision to acquire hardware and software to equip the sites upon activation. Companies can acquire and store the necessary equipment and software beforehand or can plan to acquire the hardware and software when it is needed. A key factor in the decision is whether standard systems are used that can be readily acquired when replacements are needed or are unique, specialized, outdated and therefore difficult to acquire on short notice. If companies depend on hardware that is not readily available to support critical business applications, plans must include provision to acquire the hardware in time to meet the RTO. This fact may dictate that the companies acquire the

critical components beforehand and store them so they are available when required.

Additionally, part of the recovery of IT facilities will involve telecommunications, for which the strategies usually considered include:

• Network disaster prevention, which includes:

– Alternative routing

– Diverse routing

– Long-haul network diversity

– Protection of the local loop

– Voice recovery

– Availability of appropriate circuits and adequate bandwidth

• Server disaster recovery plans

4.16.4 DEVELOPMENT OF DISASTER RECOVERY PLANS

As part of a greater business continuity planning process, IT disaster recovery planning follows the same path. After conducting a BIA and risk assessment (or determining the risk and effectiveness of mitigation controls otherwise), the IT disaster recovery strategy is developed. Implementing this strategy means making changes to:

• IT systems

• Networks

• IT processing sites

• Organization structure (headcount, roles, positions)

• IT processes and procedures

An IT DRP is a well-structured collection of processes and procedures intended to make the disaster response and recovery effort swift, efficient and effective to achieve the synergy between recovery teams. The plan should be documented and written in simple language that is understandable to all.

IT DRP Contents

Typically, the IT DRP contains:

• Procedures for declaring a disaster (escalation procedures)

• Criteria for plan activation (i.e., in which circumstances the disaster is declared, when the IT DRP is put to action, which scenarios are covered by

the plan [loss of the IT system, loss of the processing site, loss of the office])

• Linkage with the overarching plans (for instance, emergency response plan or crisis management plan or BCPs for different lines of business)

• The person (or people) responsible for each function in plan execution

• Recovery teams and their responsibilities

• Contact and notification lists (contact information for recovery teams, recovery managers, stakeholders, etc.)

• The step-by-step explanation of the whole recovery process (i.e., where and when the recovery should take place [the same site or backup site], what has to be recovered [IT systems, networks, etc.], the order of recovery)

• Recovery procedures (for each IT system or component). Note: the level of detail here greatly varies and depends on the practices used in the organization.

• Contacts for important vendors and suppliers

• The clear identification of the various resources required for recovery and continued operation of the organization

It is common to identify teams of personnel who are made responsible for specific tasks in case of disasters. Some important teams should be formed and their responsibilities are explained later in this section. Copies of the plan should be maintained offsite. The plan must be structured so that its parts can easily be handled by different teams.

IT DRP Scenarios

Although no two disasters are alike, the plan should outline which scenarios are covered, such as:

• Loss of network connectivity

• Loss of a key IT system

• Loss of the processing site (server room)

• Loss of critical data

• Loss of an office, etc.

• Loss of key service provider (e.g., cloud)

Normally, this section is quite short; however, it is important to remember that the best plan always accounts for the worst-case conditions (such as peak

of sales, end of reporting period, etc.).

Recovery Procedures

Depending on the type of disaster, the sequence of the recovery effort may vary; however, the plan should contain a simple, high-level overview of the sequence for every major disaster scenario referring to the more detailed recovery procedures.

Organization and Assignment of Responsibilities

The DRP should identify the teams with their assigned responsibilities in the event of an incident/disaster. IS and end-user personnel should be identified to go through the recovery procedures that have been developed for business/process recovery and key decision making. These individuals usually lead teams created in response to a critical function or task defined in the plan. Depending on the size of the business operation, these teams may be designated as single-person positions. The involvement of the following teams depends on the level of the disruption of service and the types of assets lost or damaged. It is a good idea to develop a matrix on the correlation between the teams needed to participate and the estimated recovery effort/level of disruption.

The recovery/continuity/response teams may include any of the following:

• **Incident response team**—This is a team that has been designated to receive the information about every incident that can be considered as a threat to assets/processes. This reporting can be useful for coordinating an incident in progress and or for postmortem analysis. The analysis of all incidents also provides input for updating the recovery plans.

• **Emergency action team**—This team includes first responders, designated fire wardens and bucket crews, whose function is to deal with fires or other emergency response scenarios. One of their primary functions is the orderly evacuation of personnel and the securing of human life.

• **Information security team**—The main mission of this team is to develop the needed steps to maintain a similar level of information and IT resource security as was in place at the primary site before the contingency and implement the needed security measures in the alternative procedures environment. Additionally, this team must continually monitor the security

of system and communication links, resolve any security conflicts that impede the expeditious recovery of the system, and assure the proper installation and functioning of security software. The team is also responsible for the security of

the organization’s assets during the disorder following a disaster.

• **Damage assessment team**—This team assesses the extent of damage following the disaster. The team should be comprised of individuals who have the ability to assess damage and estimate the time required to recover operations at the affected site. This team should include staff skilled in the use of testing equipment, knowledgeable about systems and networks, and trained in applicable safety regulations and procedures. In addition, they have the responsibility to identify possible causes of the disaster and their impact on damage and predictable downtime.

• **Emergency management team**—This team is responsible for coordinating the activities of all other recovery/continuity/response teams and handling key decision making. They determine the activation of the BCP. Other functions entail arranging the finances of the recovery, handling legal matters evolving from the disaster, and handling public relations and media inquiries. This team functions as disaster overseers and is required to coordinate the following activities:

– Retrieve critical and vital data from offsite storage.

– Install and/or test systems software and applications at the systems recovery site (hot site, cold site).

– Identify, purchase, and install hardware at the system recovery site.

– Operate from the system recovery site.

– Reroute WAN communications traffic.

– Reestablish the local area user/system network.

– Transport users to the recovery facility.

– Restore databases.

– Supply necessary office goods (e.g., special forms, check stock, paper).

– Arrange and pay for employee relocation expenses at the recovery facility.

– Coordinate systems use and employee work schedules.

• **Offsite storage team**—This team is responsible for obtaining, packaging and shipping media and records to the recovery facilities, as well as establishing and overseeing an offsite storage schedule for information

created during operations at the recovery site.

• **Software team**—This team is responsible for restoring system packs, loading and testing OSs software, and resolving system-level problems.

• **Applications team**—This team travels to the system recovery site and restores user packs and application programs on the backup system. As the recovery progresses, this team may have the responsibility of monitoring application performance and database integrity.

• **Emergency operations team**—This team consists of shift operators and shift supervisors who will reside at the systems recovery site and manage system operations during the entirety of the disaster and recovery projects.

Another responsibility might be coordinating hardware installation, if a hot site or other equipment-ready facility has not been designated as the recovery center.

• **Network recovery team**—This team is responsible for rerouting wide-area voice and data communications traffic, reestablishing host network control and access at the system recovery site, providing ongoing support for data communications, and overseeing communications integrity.

• **Communications team**—This team travels to the recovery site where they work in conjunction with the remote network recovery team to establish a user/system network. This team also is responsible for soliciting and installing communications hardware at the recovery site and working with local exchange carriers and gateway vendors in the rerouting of local service and gateway access.

• **Transportation team**—This team serves as a facilities team to locate a recovery site, if one has not been predetermined, and is responsible for coordinating the transport of company employees to a distant recovery site.

It also may assist in contacting employees to inform them of new work locations,

and scheduling and arranging employee lodgings.

• **User hardware team**—This team locates and coordinates the delivery and installation of user terminals, printers, typewriters, photocopiers and other necessary equipment. This team also offers support to the communications team and to any hardware and facilities salvage efforts.

• **Data preparation and records team**—Working from terminals that connect to the user recovery site, the team updates the applications database. This team also oversees additional data-entry personnel and assists record salvage efforts in acquiring primary documents and other

input information sources.

• **Administrative support team**—This team provides clerical support to the other teams and serves as a message center for the user recovery site. This team also may control accounting and payroll functions as well as ongoing facilities management.

• **Supplies team**—This team supports the efforts of the user hardware team by contacting vendors and coordinating logistics for an ongoing supply of necessary office and computer supplies.

• **Salvage team**—This team manages the relocation project. This team also makes a more detailed assessment of the damage to the facilities and equipment than was performed initially; provides the emergency

management team with the information required to determine whether planning should be directed toward reconstruction or relocation; provides information necessary for filing insurance claims (insurance is the primary source of funding for the recovery efforts); and coordinates the efforts necessary for immediate records salvage, such as restoring paper documents and electronic media.

• **Relocation team**—This team coordinates the process of moving from the hot site to a new location or to the restored original location. This involves relocating the IS processing operations, communications traffic and user operations. This team also monitors the transition to normal service levels.

• **Coordination team**—This team is responsible for coordinating the recovery efforts across various offices located at different geographical locations. Where

significant IT functions have been off-shored to distant geographical locations, this team acts as the focus for coordination between the organization and the third-party service providers.

• **Legal affairs team**—This team is responsible for handling the legal issues arising for various reasons due to any incident or unavailability of services (e.g., according to new laws enacted by many countries, the organization is responsible for securing its IT assets, and will be liable for damages to innocent parties in case of incidence).

• **Recovery test team**—This team is responsible for testing of various plans developed and analyzing the results.

• **Training team**—This team provides training to the users for provisions of business continuity and disaster recovery procedures.

Note: The IS auditor should have knowledge of these responsibilities; however, the CISA candidate will not be tested on these specific assignments as they vary from organization to organization.

4.16.5 DISASTER RECOVERY TESTING METHODS

Based on the risk assessment and BIA, critical applications and infrastructure are identified for testing. These should be developed into a testing schedule.

Recovery plans that have not been tested leave an organization with an unacceptable likelihood that plans will not work. As testing plans cost time and resources, an organization should carefully plan and develop test objectives to ensure that measurable benefits can be achieved. Once these objectives have been defined, an independent third party such as the IS

auditor should be present to monitor and evaluate the test. A result of the evaluation step should be a list of recommendations to improve the plan.

In summary, testing should include:

• Develop test objectives.

• Execute the test.

• Evaluate the test.

• Develop recommendations to improve the effectiveness of testing processes and recovery plans.

• Implement a follow-up process to ensure that the recommendations are implemented.

It is extremely unlikely that no recommendations will result and that everything works as planned. If it does, it is likely that a more challenging test should have been planned.

Types of Tests

The types of disaster recovery tests include:

• **Checklist review**—This is a preliminary step to a real test. Recovery checklists are distributed to all members of a recovery team to review and ensure that the checklist is current.

• **Structured walk-through**—Team members physically implement the plans on paper and review each step to assess its effectiveness, identify

enhancements, constraints and deficiencies.

• **Simulation test**—The recovery team role play a prepared disaster scenario without activating processing at the recovery site.

• **Parallel test**—The recovery site is brought to a state of operational readiness, but operations at the primary site continue normally.

• **Full interruption test**—Operations are shut down at the primary site and shifted to the recovery site in accordance with the recovery plan; this is the most rigorous form of testing but is expensive and potentially disruptive.

Testing should start simply and increase gradually, stretching the objectives and success criteria of previous tests so as to build confidence and minimize risk to the business. **Figure 4.36** shows how tests can become progressively more challenging.

Most recovery tests fall short of a full-scale test of all operational portions of the corporation. This should not preclude performing full or partial testing because one of the purposes of the disaster recovery test is to determine how well the plan works or which portions of the plan need improvement.

Surprise tests are advantageous because they are similar to real-life incident response situations. However, they can be terribly disruptive to production and operations and can alienate individuals who are in some way disrupted by them. The test should be scheduled during a time that will minimize disruptions to normal operations, such as long weekends. It is important that the key recovery team members are involved in the test process and are allotted the necessary time to devote their full effort. The test should address all critical components and simulate actual prime-time processing conditions, even if the test is conducted during off hours. Ideally, full-interruption tests should be performed annually after individual plans have been tested separately with satisfactory results.

Testing

The test should strive to accomplish the following tasks:

• Verify the completeness and precision of the response and recovery plan.

• Evaluate the performance of the personnel involved in the exercise.

• Appraise the demonstrated level of training and awareness of individuals who are not part of the recovery/response team.

• Evaluate the coordination among the team members and external vendors and suppliers.

• Measure the ability and capacity of the backup site to perform prescribed processing.

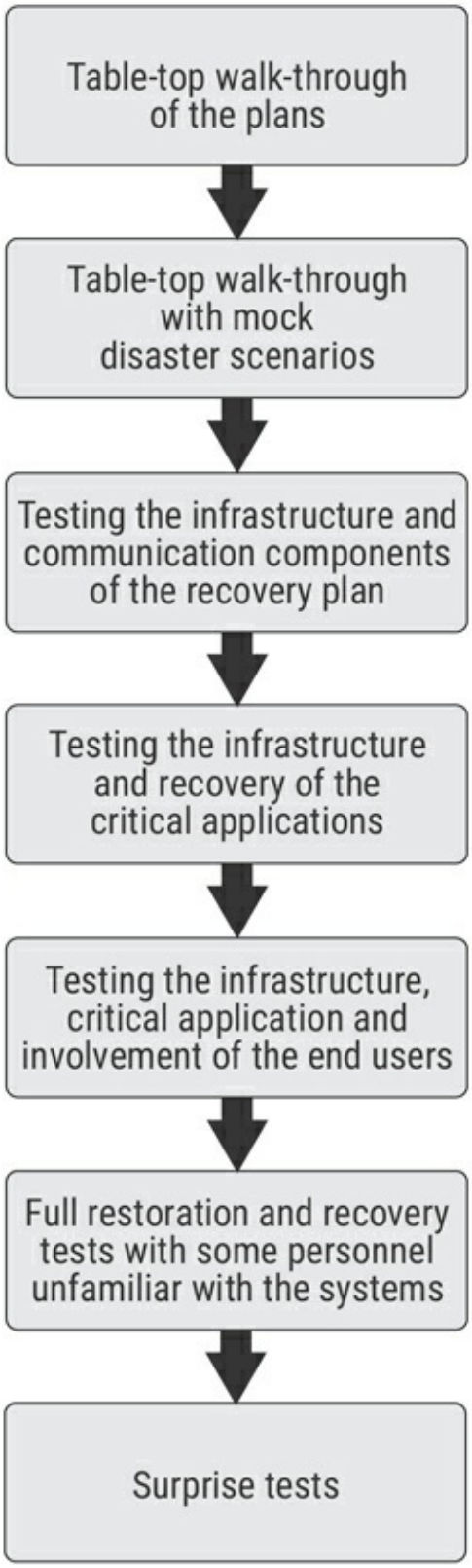
• Assess the vital records retrieval capability.

• Evaluate the state and quantity of equipment and supplies that have been relocated to the recovery site.

• Measure the overall performance of operational and information systems

processing activities related to maintaining the business entity.

Figure 4.36—Progression of Disaster Recovery Tests



To perform testing, each of the following phases should be completed:

• **Pretest**—The pretest consists of the set of actions necessary to set the stage for the actual test, including transporting and installing required backup equipment, gaining access to the recovery site, accessing recovery documentation, etc.

• **Test**—The test is the real action of the disaster recovery test. Actual operational activities are executed to test the specific objectives of the plan.

Applications are failed over; data entry and business processing should take place. Evaluators should review staff members as they perform the designated tasks. This is the actual test of preparedness to respond to an emergency.

• **Posttest**—The posttest is the cleanup of group activities. This phase comprises assignments, such as restoring the applications back to the primary location and returning all resources to their proper place, disconnecting equipment, returning personnel to their normal locations, and deleting all company data from third-party systems. The posttest cleanup also includes formally evaluating the plan and implementing indicated improvements. During every phase of the test, detailed documentation of observations, problems and resolutions should be maintained. Each team should have a diary with specific steps and information recorded. This documentation serves as important historical information that can facilitate actual recovery during a real disaster. The documentation also aids in performing detailed analysis of the strengths and weaknesses of the plan.

Test Results

Metrics should be developed and used in measuring the success of the plan and testing against the stated objectives. Results should be recorded and evaluated quantitatively, as opposed to an evaluation based only on verbal descriptions. The resulting metrics should be used not only to measure the effectiveness of the plan, but more important, to improve it. Although specific measurements vary depending on the test and the organization, the following types of metrics usually apply:

• **Time**—Elapsed time for completion of prescribed tasks. This is essential to refine the response time estimated for every task in the escalation process.

Was the RTO met?

• **Data**—Were all data required data recovered? Was the RPO met? Was the recovery point aligned (where required) across all inter-connected applications?

• **Amount**—Amount of work performed at the backup site by clerical personnel and the amount of information systems processing operations.

Does the recovery site allow the required throughput?

• **Percentage and/or number**—The number of critical systems successfully recovered can be measured with the number of transactions processed.

• **Accuracy**—Accuracy of the data entry at the recovery site versus normal accuracy (as a percentage). The accuracy of actual processing cycles can be determined by comparing output results with those for the same period processed under normal conditions.

4.16.6 INVOKING DISASTER RECOVERY PLANS

The BCP and DRP should be very closely aligned. As noted in section 4.15, Business Continuity Plan, a designated individual should be notified of all relevant incidents as soon as any triggering event occurs. This person should then follow a preestablished escalation protocol (e.g., calling in a spokesperson, alerting top management and involving regulatory agencies), which may be followed by invoking a recovery plan, such as the information technology DRP.

The required teams (discussed earlier in this section) should be then be mobilized with the incident evaluated to confirm which of the tested scenarios it most closely resembles. Examples include:

• Loss of network connectivity

• Loss of a key IT system

• Loss of the processing site (server room)

• Loss of critical data

• Loss of an office, etc.

• Loss of key service provider (e.g., cloud)

Note that there may be more than one way to respond to a given incident.

These should be evaluated with those most likely to deliver the required RPO

and RTO selected. The documented recovery procedures should then be followed. It should be noted that recovery procedures may not include all

required recovery steps as the testing may not have been comprehensive or the selected scenario an exact match. In such incidents the response teams may need to evaluate their options at each step. All decisions made should be documented and used to update the recovery procedures after normal service has been achieved.

CASE STUDY

An IS auditor has been asked to represent the internal audit department of her organization on a task force to define the requirements for a new branch automation project for a Pinkwater Bank, a community bank with 16

branches. This new system would handle deposit and loan information and other confidential customer information.

The branches are located within the same geographic area, so the director of branch operations has suggested the use of a microwave radio system to provide connectivity, due to its low cost of operation and the fact that it is a private (and not a public) network. The director has also strongly suggested that it would be preferable to provide each branch with a direct coaxial connection to the Internet (using the local cable television provider) as a backup if the microwave system develops a fault.

The direct Internet connection would also be connected to a wireless access point at each branch to provide free wireless access to customers. The director also asked that each branch be provided with mail and application servers that would be administered by the administrative manager of each branch. The IS auditor was informed by the IT manager for the bank that the cable service provider will encrypt all traffic sent over the direct coaxial connection to the Internet.

1.

In reviewing the information for this project, what would be the **MOST**

important concern regarding the use of microwave radio systems based on the above scenario?

A. Susceptibility for interception of transmitted data

B. Lack of available data transmission encryption solutions

C. Likelihood of a service outage

D. Cost overruns in implementation

2.

Which of the following would **BEST** reduce the likelihood of business systems being successfully attacked from the public internet through the wireless network?

A. Scanning all connected devices for malware

B. Segmenting internal network & public internet access though a firewalled subnet

C. Logging all access and issuing alerts for failed logon attempts D. Limiting all network access to regular business hours and standard protocols

Pinkwater Bank is now developing revised BCPs and DRPs for its

headquarters facility and network of 16 branch offices. The current plans have not been updated in more than eight years, during which time the organization has grown by over 300 percent. At the headquarters facility, there are approximately 750 employees. These individuals connect over a LAN to an array of more than 60 application, database and file print servers that are located in the corporate data center and over a frame relay network to the branch offices. Traveling users access corporate systems remotely by connecting over the Internet using VPN. Users at both headquarters and the branch offices access the Internet through a firewall and proxy server located in the data center.

Critical applications have an RTO of between three and five days. Branch offices

are located between 30 and 50 miles from one another, with none closer than 25 miles to the headquarters' facility. Each branch office has between 20 and 35 employees plus a mail server and a file/print server.

Backup media for the data center are stored at a third-party facility that is 35

miles away. Backups for servers located at the branch offices are stored at nearby branch offices using reciprocal agreements between offices.

Current contracts with a third-party hot site provider include 25 servers, work area space equipped with desktop computers to accommodate 100

individuals, and a separate agreement to ship up to two servers and 10

desktop computers to any branch office declaring an emergency. The contract term is for three years, with equipment upgrades occurring at renewal time.

The hot site provider has multiple facilities throughout the country in case the primary facility is in use by another customer or rendered unavailable by the disaster. Senior management desires that any enhancements be as cost effective as possible.

3.

When negotiating new contracts with the vendor, which of the

following should the IS auditor recommend to management concerning the hot site in this situation?

A. Desktops at the hot site should be increased to 750.

B. An additional 35 servers should be added to the hot site contract.

C. All backup media should be stored at the hot site to shorten the RTO.

D. Desktop and server equipment requirements should be reviewed

quarterly.

4.

When negotiating new contracts with the vendor, which of the

following should the IS auditor recommend to management concerning branch office recovery?

A. Add each of the branches to the existing hot site contract.

B. Ensure branches have sufficient capacity to back each other up.

C. Relocate all branch mail and file/print servers to the data center.

D. Add additional capacity to the hot site contract equal to the largest branch.

ANSWERS TO CASE STUDY QUESTIONS

1.

A.

Lack of encryption is the most important concern since

microwave radio systems are easy to tap.

B.

Lack of scalability is important but not as important as ensuring the confidentiality and integrity of customer data.

C.

Likelihood of a service outage is important but not as important as ensuring the confidentiality and integrity of customer data.

D.

Cost overruns in implementation are important but not as

important as ensuring the confidentiality and integrity of customer data.

2.

A.

Scanning for malware would not detect the use of investigative tools designed to harvest passwords or reveal network vulnerabilities.

B.

Isolating the wireless network by placing it on a firewalled subnet would best reduce the likelihood of attack.

C.

Logging access would not prevent a successful attack.

D.

Limiting access to normal business hours would not prevent a successful attack.

3.

A.

Because not all employee job functions are critical during a disaster, it is not necessary to contact the same number of desktops at a recovery facility as the number of employees.

B.

Similarly, not every server is critical to the continued operation of the business. Only a subset will be required.

C.

Because there is no assurance that the hot site will not already be occupied, it would not be advisable to store backup media at the facility. These facilities are generally not designed to provide extensive media storage, and frequent testing by other customers could compromise the security of the media.

D.

As equipment needs in a rapidly growing business are subject

to frequent change, quarterly reviews are necessary to ensure that the recovery capability keeps pace with the organization.

4.

A.

Adding each of the branches to the hot site contract would be far more expensive.

B.

The most cost-effective solution is to recommend that

branches have sufficient capacity to accommodate critical

personnel from another branch. Because critical job functions would represent only perhaps 20 percent of the staff from the affected branch, accommodations for only four to seven

critical staff members would be needed.

C.

Relocating branch servers to the data center could result in

performance issues and would not address the question of where

to locate displaced employees.

D.

Adding capacity to the hot site contract would not provide

coverage as hot site contracts base their pricing on each location covered.

Chapter 5:

Protection of Information Assets

Overview

Domain 5 Exam Content Outline

Learning Objectives/Task Statements

Suggested Resources for Further Study

Self-assessment Questions

Answers to Self-Assessment Questions

Part A: Information Asset Security and Control

5.0

Introduction

5.1

Information Asset Security Frameworks, Standards and Guidelines 5.2

Privacy Principles

5.3

Physical Access and Environmental Controls

5.4

Identity and Access Management

5.5

Network and End-point Security

5.6

Data Classification

5.7

Data Encryption and Encryption-related Techniques

5.8

Public Key Infrastructure

5.9

Web-based Communication Technologies

5.10 Virtualized Environments

5.11 Mobile, Wireless and Internet-of-things Devices

Part B: Security Event Management

5.12 Security Awareness Training and Programs 5.13 Information System Attack Methods and Techniques

5.14 Security Testing Tools and Techniques

5.15 Security Monitoring Tools tand Techniques

5.16 Incident Response Management

5.17 Evidence Collection and Forensics

Case Study

Case Study

Answer to Case Study Questions

OVERVIEW

This chapter addresses the key components that ensure confidentiality, integrity and availability (CIA) of information assets. The design, implementation and monitoring of logical and physical access controls are explained. Network infrastructure security, environmental controls, and processes and procedures used to classify, enter, store, retrieve, transport and dispose of confidential information assets are covered. The methods and procedures that organizations follow are described, focusing on the auditor's role in evaluating these procedures for suitability and effectiveness.

This domain represents 27 percent of the CISA examination (approximately 41 questions).

DOMAIN 5 EXAM CONTENT OUTLINE

Part A: Information Asset Security and Control

1. Information Asset Security Frameworks, Standards, and Guidelines 2. Privacy Principles

3. Physical Access and Environmental Controls

4. Identity and Access Management

5. Network and End-point Security

6. Data Classification

7. Data Encryption and Encryption-related Techniques

8. Public Key Infrastructure (PKI)

9. Web-based Communication Technologies

10. Virtualized Environments

11. Mobile, Wireless, and Internet-of-Things (IOT) Devices

Part B: Security Event Management

1. Security Awareness Training and Programs
2. Information System Attack Methods and Techniques
3. Security Testing Tools and Techniques
4. Security Monitoring Tools and Techniques

5. Incident Response Management

6. Evidence Collection and Forensics

LEARNING OBJECTIVES/TASK STATEMENTS

Within this domain, the IS auditor should be able to:

• Conduct audit in accordance with IS audit standards and a isk-based IS

audit strategy. (T2)

• Evaluate problem and incident management policies and practices. (T26)

• Evaluate the organization's information security and privacy policies and practices. (T29)

• Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded. (T30)

• Evaluate logical security controls to verify the confidentiality, integrity, and availability of information. (T31)

• Evaluate data classification practices for alignment with the organization's policies and applicable external requirements. (T32)

• Evaluate policies and practices related to asset life cycle management.

(T33)

• Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives. (T34)

• Perform technical security testing to identify potential threats and vulnerabilities. (T35)

• Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices. (T39)

SUGGESTED RESOURCES FOR FURTHER STUDY

Davis, Chris; Mike Schiller; Kevin Wheeler; *IT Auditing: Using Controls to Protect Information Assets, 2nd Edition*, McGraw Hill, USA, 2011

Harris, Shon; Allen Harper; Chris Eagle; Jonathan Ness; Gideon Lenkey; Terron Williams; *Gray Hat Hacking: The Ethical Hackers Handbook, 3rd Edition*, McGraw Hill, USA, 2011

ISACA, *The Business Model for Information Security*, USA, 2010

ISACA, Cloud Computing Guidance, *https://www.isaca.org/Knowledge-Center/Research/Pages/Cloud.aspx*

ISACA, COBIT® 2019, USA, 2018, *www.isaca.org/cobit*

ISACA, ISACA Innovation Insights, *https://www.isaca.org/Knowledge-Center/Research/Pages/isaca-innovation-insights.aspx*

ISACA, *Security Considerations for Cloud Computing*, USA, 2013, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Security-Considerations-for-Cloud-Computing.aspx*

ISACA, ISACA Tech Briefs, *https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ISACA-Tech-Briefs.aspx*

International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 27002:2013, *Information technology—Security techniques—Code of practice for information security controls*, Switzerland, 2013, *www.iso.org/standard/54533.html*

McClure, Stuart; Joel Scambray; George Kurtz; *Hacking Exposed 7: Network Security Secrets & Solution* s, McGraw Hill, USA, 2012

Peltier, Thomas R.; *Information Security Risk Analysis, 3rd Edition*, Auerbach Publications, USA, 2010

Stamp, Mark; *Information Security: Principles and Practice, 2nd Edition*, John Wiley & Sons, USA, 2011

SELF-ASSESSMENT QUESTIONS

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often a question will require the candidate to choose the

MOST likely or **BEST** answer among the options provided. Please note that these questions are not actual or retired exam items. Please see the section

"About This Manual" for more guidance regarding practice questions.

5-1

An IS auditor reviewing the configuration of a signature-based

intrusion detection system would be **MOST** concerned if which of the following is discovered?

A. Auto-update is turned off.

B. Scanning for application vulnerabilities is disabled.

C. Analysis of encrypted data packets is disabled.

D. The IDS is placed between the demilitarized zone and the firewall.

5-2

Which of the following **BEST** provides access control to payroll data being processed on a local server?

A. Logging access to personal information

B. Using separate passwords for sensitive transactions

C. Using software that restricts access rules to authorized staff D. Restricting system access to business hours

5-3

An IS auditor has just completed a review of an organization that has a mainframe computer and two database servers where all production data reside. Which of the following weaknesses would be considered the **MOST** serious?

A. The security officer also serves as the database administrator.

B. Password controls are not administered over the two database

servers.

C. There is no business continuity plan for the mainframe system’s noncritical applications.

D. Most local area networks do not back up file-server-fixed disks regularly.

5-4

An organization is proposing to install a single sign-on facility giving access to all systems. The organization should be aware that:

A. maximum unauthorized access would be possible if a password is disclosed.

B. user access rights would be restricted by the additional security parameters.

C. the security administrator’s workload would increase.

D. user access rights would be increased.

5-5

When reviewing an implementation of a Voice-over Internet Protocol system over a corporate wide area network, an IS auditor should expect to find:

A. an integrated services digital network data link.

B. traffic engineering.

C. wired equivalent privacy encryption of data.

D. analog phone terminals.

5-6

An insurance company is using public cloud computing for one of its critical applications to reduce costs. Which of the following would be of **MOST** concern to the IS auditor?

A. The inability to recover the service in a major technical failure scenario

B. The data in the shared environment being accessed by other

companies

C. The service provider not including investigative support for

incidents

D. The long-term viability of the service if the provider goes out of business

5-7

Which of the following **BEST** determines whether complete encryption and authentication protocols for protecting information while being

transmitted exist?

A. A digital signature with RSA has been implemented.

B. Work is being done in tunnel mode with the nested services of authentication header (AH) and encapsulating security payload

(ESP).

C. Digital certificates with RSA are being used.

D. Work is being done in transport mode with the nested services of AH and ESP.

5-8

Which of the following concerns about the security of an electronic message would be addressed by digital signatures?

A. Unauthorized reading

B. Theft

C. Unauthorized copying

D. Alteration

5-9

Which of the following characterizes a distributed denial-of-service attack?

A. Central initiation of intermediary computers to direct simultaneous spurious message traffic at a specified target site

B. Local initiation of intermediary computers to direct simultaneous spurious message traffic at a specified target site

C. Central initiation of a primary computer to direct simultaneous spurious message traffic at multiple target sites

D. Local initiation of intermediary computers to direct staggered spurious message traffic at a specified target site

5-10

Which of the following is the **MOST** effective preventive antivirus control?

A. Scanning email attachments on the mail server

B. Restoring systems from clean copies

C. Disabling universal serial bus ports

D. An online antivirus scan with up-to-date virus definitions

ANSWERS TO SELF-ASSESSMENT QUESTIONS

5-1

A.

The most important aspect in a signature-based intrusion

detection system (IDS) is its ability to protect against known (signature) intrusion patterns. Such signatures are provided

by the vendor and are critical to protecting an enterprise

from outside attacks.

B.

One of the key disadvantages of IDS is its inherent inability to scan for vulnerabilities at the application level.

C.

An IDS cannot break encrypted data packets to identify the

source of the incoming traffic.

D.

A demilitarized zone is an internal network segment in which

systems (e.g., a web server) accessible to the public are housed.

In order to provide the greatest security and efficiency, an IDS

should be placed behind the firewall so that it will detect only those attacks/intruders that enter the firewall.

5-2

A.

Logging access to personal information is a good control in that it will allow access to be analyzed if there is concern of

unauthorized access. However, it will not prevent access.

B.

Restricting access to sensitive transactions will restrict access only to some of the data. It will not prevent access to other data.

C.

The server and system security should be defined to allow

only authorized staff members access to information about

the staff whose records they handle on a day-to-day basis.

D.

System access restricted to business hours only restricts when

unauthorized access can occur and would not prevent such access

at other times. It is important to consider that the data owner is responsible for determining who is allowed access via the written software access rules.

5-3

A.

The security officer serving as the database administer, while a

control weakness, does not carry the same disastrous impact as the absence of password controls.

B.

The absence of password controls on the two database

servers, where production data reside, is the most critical

weakness.

C.

Having no business continuity plan for the mainframe system’s

noncritical applications, while a control weakness, does not carry the same disastrous impact as the absence of password controls.

D.

Most local area networks not backing-up regularly, while a

control weakness, does not carry the same disastrous impact as

the absence of password controls.

5-4

A.

If a password is disclosed when single sign-on is enabled,

there is a risk that unauthorized access to all systems will be possible.

B.

User access rights should remain unchanged by single sign-on, as additional security parameters are not implemented necessarily.

C.

One of the intended benefits of single sign-on is the simplification of security administration.

D.

One of the intended benefits of single sign-on is the unlikelihood of an increased workload.

5-5

A.

The standard bandwidth of an integrated services digital network data link would not provide the quality of services required for corporate Voice-over Internet Protocol (VoIP) services.

B.

To ensure that quality of service requirements are achieved,

the VoIP service over the wide area network should be

protected from packet losses, latency or jitter. To reach this objective, the network performance can be managed to

provide quality of service and class of service support using statistical techniques, such as traffic engineering.

C.

Wired equivalent privacy is an encryption scheme related to

wireless networking.

D.

The VoIP phones are usually connected to a corporate local area

network and are not analog.

5-6

A.

Benefits of cloud computing are redundancy and the ability to

access systems and data in the event of a technical failure.

B.

Considering that an insurance company must preserve the

privacy/confidentiality of customer information,

unauthorized access to information and data leakage are the

major concerns.

C.

The ability to investigate an incident is important, but most

important is addressing the risk of an incident—the exposure of

sensitive data.

D.

If a cloud provider goes out of business, the data should still be available from backups.

5-7

A.

A digital signature provides authentication and integrity.

B.

Tunnel mode provides encryption and authentication of the

complete IP package. To accomplish this, the authentication

header and encapsulating security payload services can be

nested.

C.

A digital certificate provides authentication and integrity.

D.

The transport mode provides primary protection for the protocols’

higher layers; that is, protection extends to the data field

(payload) of an IP package.

5-8

A.

Digital signatures will not identify, prevent or deter unauthorized reading.

B.

Digital signatures will not identify, prevent or deter theft.

C.

Digital signatures will not identify, prevent or deter unauthorized copying.

D.

A digital signature includes an encrypted hash total of the

size of the message as it was transmitted by its originator.

This hash would no longer be accurate if the message was

altered subsequently, indicating that the alteration had

occurred.

5-9

A.

This best describes a distribute denial-of-service (DDoS)

attack. Such attacks are centrally initiated and involve the use of multiple compromised computers. The attacks work by

flooding the target site with spurious data, thereby overwhelming the network and other related resources. To

achieve this objective, the attacks need to be directed at a

specific target and occur simultaneously.

B.

DDoS attacks are not locally initiated.

C.

DDoS attacks are not initiated using a primary computer.

D.

DDoS attacks are not staggered.

5-10 A.

Scanning email attachments on the mail server is a preventive

control. It will prevent infected email files from being opened by the recipients, which would cause their machines to become

infected.

B.

Restoring systems from clean copies is a preventive control. It

will ensure that viruses are not introduced from infected copies or backups, which would reinfect machines.

C.

Disabling universal serial bus (USB) ports is a preventive control.

It prevents infected files from being copied from a USB drive

onto a machine, which would cause the machine to become

infected.

D.

Antivirus software can be used to prevent virus attacks. By

running regular scans, it can also be used to detect virus

infections that have already occurred. Regular updates of the software are required to ensure it is able to update, detect and treat viruses as they emerge.

PART A: INFORMATION ASSET SECURITY

AND CONTROL

5.0 INTRODUCTION

Protection of information assets includes the key components that ensure confidentiality, integrity and availability (CIA) of information assets. Many of the topics covered in this chapter may, on the surface, seem very familiar to candidates; however, it is important to note that the topics addressed in this chapter require a thorough knowledge of the technologies used and the potential control weaknesses that can be exploited by attackers. CISA candidates should be fully aware of and conversant with the components of network infrastructure security, logical access issues and the key elements of information security management.

Information security is an essential component of governance and management that affects all aspects of entity-level controls. Audit professionals include appropriate information security evaluations throughout their audit work. The information security management function is responsible for the governance, policy, enforcement, monitoring and innovation necessary for the modern business to establish cost-effective information security processes, while providing adequate information security assurance within the risk appetite and budget of the organization.

5.1 INFORMATION ASSET SECURITY FRAMEWORKS,

STANDARDS AND GUIDELINES

Many industries have standards that may be used as a benchmark for security

across the industry sector. One example is the Payment Card Industry Data Security Standard (PCI DSS), which is used as a standard for all organizations that process payment cards (e.g., debit cards and credit cards).

This is an example of an industry standard, but compliance is not required by

law. Such standards are found in many industries including health care, accounting, audit and telecommunications. In some industries, such as electrical power, regulations require compliance with a standard. To meet the requirements of the standard, a framework is often used to describe how an organization can achieve compliance.

A control framework is a set of fundamental controls that helps support and protect an enterprise by preventing/minimizing financial or information loss and adding/preserving value.

The selection of controls requires the evaluation and implementation of the right control in the right way. Based on data collected through an analysis method (e.g., cost-benefit, return on investment [ROI] and risk assessment results), management will decide on the best available control, or group of controls, to mitigate a specific risk. However, a poorly implemented control may pose a significant risk to the organization by creating a false sense of security or leading to a denial of service if the control does not function correctly. The implementation of a technical control requires that the control is surrounded by proper procedures, the personnel who operate it are adequately trained, a person is assigned ownership of the control (often the person who owns the risk), and the control is monitored and tested to ensure its correct operation and effectiveness.

5.1.1 AUDITING THE INFORMATION SECURITY

MANAGEMENT FRAMEWORK

Auditing the information security framework of an organization involves the audit of logical access, the use of techniques for testing security and the use of investigation techniques. The information security management framework should be reviewed per the basic elements in an information security framework. Additional areas of concern are risk management, risk assessment results, control design and incident management among other areas.

Reviewing Written Policies, Procedures and Standards

Policies and procedures provide the framework and guidelines for maintaining proper operation and control. The IS auditor should review the

policies and procedures to determine if they set the tone for proper security and provide a means for assigning responsibility for maintaining a secure information systems environment. This policy review should also include reviewing the date of the last update to ensure that documents remain current and meet organizational information security needs.

Formal Security Awareness and Training

Effective security will always be dependent on people. As a result, security can only be effective if employees know what is expected of them and their responsibilities. They should know why various security measures, such as locked doors and use of logon IDs, are in place and the repercussions of violating security.

Promoting security awareness is a preventive control. Through this process, employees become aware of their responsibilities for maintaining good physical and logical security. This can also be a detective measure, because it encourages people to identify and report possible security violations.

Training should start with the new employee orientation process. Ongoing awareness includes articles in company newsletters, visible and consistent security enforcement and short reminders during staff meetings. The security administrator should direct the program. To determine the effectiveness of the program, the IS auditor should interview a sample of employees to determine their overall awareness.

See section 5.12, Security Awareness Training and Programs, for more information.

Data Ownership

Data ownership refers to the classification of data elements and the allocation of responsibility for ensuring that they are kept confidential, complete and accurate. A key point of ownership is that, by assigning responsibility for protecting data to particular employees, accountability is established. The IS

auditor can use this information to determine if proper ownership has been assigned and whether the data owner is aware of the assignment. The IS

auditor should also review a sample of job descriptions to ensure that

responsibilities and duties are consistent with the information security policy.

The auditor should review the classification of data and evaluate their appropriateness, as they relate to the area under review.

Responsibilities include identifying and classifying data based on associated risk, authorizing access to data, review access controls, determine protection mechanism for data owned by them. In short data owners are responsible for security of data throughout life cycle of data - origination till destruction.

Data Owners

Data owners are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rules for the data for which they are responsible.

Data Custodians

Data custodians are responsible for storing and safeguarding the data and include IS personnel, such as systems analysts and computer operators.

Security Administrator

Security administrators are responsible for providing adequate physical and logical security for IS programs, data and equipment. (The physical security may be handled by someone else, not always by the security administrator.) Normally, the information security policy will provide the basic guidelines under which the security administrator will operate.

New IT Users

New IT users (employees or third parties) and, in general, all new users who are assigned PCs or other IT resources should sign a document stating the main IT

security obligations that they are thereby engaged to know and observe. These obligations are:

• Read and agree to follow security policies.

• Keep logon IDs and passwords secret.

• Create quality passwords according to policy.

• Lock terminal screens when not in use.

• Report suspected violations of security.

• Maintain good physical security—keep doors locked, safeguard access keys, do not disclose access door lock combinations and question unfamiliar people.

• Conform to applicable laws and regulations.

• Use IT resources only for authorized business purposes.

Data Users

Data users include internal and the external user communities. Their levels of access should be authorized by the data owners and restricted and monitored by the security administrator. Their responsibilities regarding security are to be vigilant regarding the monitoring of unauthorized people in the work areas and comply with general security guidelines and policies.

Documented Authorizations

Data access should be identified and authorized in writing. The IS auditor can review a sample of these authorizations to determine if the proper level of written authority was provided. If the facility practices data ownership, only the data owners provide written authority.

Terminated Employee Access

Termination of employment can occur in the following circumstances:

• On the request of the employee (voluntary resignation from service)

• Scheduled (retirement or completion of contract)

• Involuntary (forced by management in special circumstances)

In case of involuntary termination of employment, the logical and physical access rights of employees to the IT infrastructure should either be withdrawn completely or highly restricted as early as possible, before the employee becomes aware of the termination or its likelihood. This ensures that terminated employees cannot continue to access potentially confidential or damaging information from the IT resources or perform any action that would result in damage of any kind to the IT infrastructure, applications and data. Similar procedures should be in place to terminate access for third parties upon terminating their activities with the organization.

When it is necessary for employees to continue to have access, such access must be monitored carefully and continuously and should take place with senior management's knowledge and authorization.

In case of voluntary or scheduled termination of employment, it is management's prerogative to decide whether access is restricted or withdrawn. This depends on:

• The specific circumstances associated with each case

• The sensitivity of the employee's access to the IT infrastructure and resources

• The requirements of the organization's information security policies, standards and procedures

See section 2.9, IT Resource Management, for more information.

Security Baselines

A baseline security plan is meant to be used as a first step to IT security. The baseline plan should be followed with a full security evaluation and plan.

Figure 5.1 illustrates baseline security topics and their associated recommendations.

Figure 5.2 shows a checklist for a baseline security evaluation.

Access Standards

Access standards should be reviewed by the IS auditor to ensure they meet organizational objectives for separating duties, prevent fraud or error, and meet policy requirements for minimizing the risk of unauthorized access.

Figure 5.1–IT Security Baseline Recommendations

Topics

Objective

Recommendations

Inventory

Establish and maintain an inventory

Users are expected to follow standards

for managing computers connected to the

network and have registered network

addresses. The OS and owner should be

included along with the data provided.

Malware

Install antivirus software with automatic

Antivirus software with an automatic

updating

DAT file should be updated at regular

intervals—no less than weekly.

Passwords

Recognize the importance of passwords

Users must use only strong passwords. The IT department should provide password guidance. Departmental accounts are created for workgroups to prevent/avoid password sharing.

Patching

Make it automatic—less work

Each machine should be configured to necessary, less chance for compromise patch automatically for OS and basic software patching. A process should be set up that works for the department and minimizes disruptions at inconvenient times. Workstations should be more automated to enable system administrators the time to give servers the attention required to minimize the impact on services offered.

Minimizing

Eliminate unnecessary services—

To improve basic security and minimize
services
reducing security risk and saving time in
effort to maintain systems, workstations
offered by
the long run
should offer only needed services. Many
systems
OSs are installed with services turned on.
By removing services, a workstation’s
chances of being compromised are
reduced and security risk is minimized.
Addressing
Eliminate many vulnerabilities with
System compromises can be time-
vulnerabilities
good system administration
consuming and damage credibility and
the business’s integrity. Information
from enterprisewide scans helps to
identify vulnerabilities on each system

and provide a baseline for comparison

when system integrity is in question.

Backups

Allow easy recovery from user mistakes

Backups should be made offsite for

and hardware failure with backups

increased security.

Figure 5.2—Baseline Security Evaluation Checklist

Topics

Evaluation Questions

Environment/inventory

• What types of data are maintained by the enterprise (e.g., financial, statistical, graphical)?

• In what form are they maintained (e.g., spreadsheets, databases)?

• Is there any critical or confidential information maintained or handled? If so, how is it protected?

• Are there any specific requirements for handling data? (legal or regulatory requirements)

• Do any machines store or require access to confidential

information?

• What type of operating systems exist?

• How many subnets exist?

• How many workstations/servers exist?

• In how many locations is there IT infrastructure?

• Has the wireless infrastructure been deployed? How is it secured?

• Is staff instructed on how to lock workstations when they step away?

• Are users aware that unexpected email attachments should not be opened?

• Is staff aware that many compromises are due to social engineering and the sharing of information?

• Does the enterprise have a network diagram that includes IP

addresses, room numbers and responsible parties?

• Has the enterprise limited and secured physical and remote access to network services?

• Is corporate hardware upgraded at regular intervals?

• Does the enterprise have a current documented inventory of

hardware and software?

• Is all corporate software licensed?

• Is license documentation available (licenses, purchase orders) if a software audit is required?

Antivirus

• Does the enterprise have an antivirus policy?

• Are all workstations running the latest version of antivirus

software, the scanning engine and the virus signature file?

• Are DAT files downloaded automatically or manually? If

manually, how often and why?

• Does staff know whom to contact when a virus is found?

• Does the antivirus system have a way to defend against zero-day attacks?

Passwords

• Is there a corporate policy requiring strong passwords?

• Is the enterprise using software that enforces strong passwords?

• Is password caching disabled on all workstations?

• Are passwords changed? If so, how often?

• Are employees aware that passwords and accounts are not to be

shared?

• Does the system administrator have written authorization to check for weak passwords?

Patching

• Are software patches applied to all operating systems automatically when possible? If done manually, how often?

• Are patches applied to web browsers and applications? If yes, how frequently?

• Do you back up each machine before applying a patch?

• Do you test patches prior to applying?

• Does the department have a documented process for patching?

• Are there sufficient sources and subscriptions to be aware of

patches to all relevant hardware and software?

Minimizing services offered

• Have you identified services that each user needs to accomplish job by systems

assignments?

• Have you removed unnecessary services that were installed by default?

• Does the technical staff review security settings and policies?

• Have you identified what services your systems are offering?

• Have you taken security measures for remote access?

• Have you transitioned to secure services?

Addressing

• Have you resolved vulnerabilities discovered by enterprisewide vulnerabilities/auditing

scans?

• Who is the contact for vulnerability scans?

• Does the IT staff complete an independent vulnerability scan for the enterprise?

• Has the enterprise deployed any form of firewalls or intrusion detection system (IDS) (host or network-based)? Are any under

consideration?

Backup and

• Are files regularly backed up?

recovery/business continuity

• Are files kept onsite in a secure location?

• Are backup files sent offsite to a physically secure location?

• Are backup files periodically restored as a test to verify whether they are a

viable alternative?

• Can you ensure that any forms of media containing confidential and sensitive information are sanitized before disposal?

• Is there redundant hardware to allow work to continue in the event of a single hardware failure?

• Does the enterprise have the ability to continue to function if central services is not available?

• Does the enterprise have the ability to continue to function in the event of a wide area network failure?

• Have you responded to and recovered from any abuse

issues/incidents?

IT staff

• How many IT staff are employed full-time/part-time?

• Does each IT staff member have a current job description?

• Do job descriptions and evaluations include IT security duties?

• Does the department have sufficient documentation to ease the

transition of incoming/outgoing staff?

• Does the enterprise have a privacy policy?

• Are all staff aware of privacy considerations?

• Are management/department users aware of the types of

(private/nonpublic) information available to systems

administrators?

• Does the enterprise have a privacy policy to address this privileged information

(confidentiality agreement/nondisclosure agreement)?

• Does the enterprise have a firewall or IDS, or other software for network diagnosis?

• Does the enterprise have tools requiring privileges and access to confidential information acquired via routers, switches, IDS,

firewalls, etc.?

Standards for security may be defined:

• At a generic level (e.g., all passwords must be at least eight characters long)

• For specific machines (e.g., all UNIX machines can be configured to enforce password changes)

• For specific application systems (e.g., sales ledger clerks can access menus that allow entry of sales invoices but may not access menus that allow check authorization)

5.2 PRIVACY PRINCIPLES

Privacy is a significant aspect of an IS auditor's role, especially in light of global regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and

Accountability Act (HIPAA) in the United States. Privacy is the right of an individual to trust that others will appropriately and legitimately use, store, share and dispose of his/her associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived. It is an important matter that, by its nature, requires a consistent approach throughout the organization. Good practice to ensure this includes:

• Privacy should be considered from the outset and be built in by design. It should be systematically built into policies, standards and procedures from the beginning.

• Private data should be collected fairly in an open, transparent manner. Only the data required for the purpose should be collected in the first instance.

• Private data should be kept securely throughout their life cycle.

• Private data should only be used and/or disclosed for the purpose for which they were collected.

• Private data should be accurate, complete and up to date.

• Private data should be deleted when they are no longer required.

To best meet these challenges, management should perform a privacy impact analysis. IS auditors may be asked to support or perform this review. Such assessments should:

• Pinpoint the nature of personally identifiable information associated with business processes.

• Document the collection, use, disclosure and destruction of personally identifiable information.

• Ensure that accountability for privacy issues exists.

• Identify legislative, regulatory and contractual requirements for privacy.

• Be the foundation for informed policy, operations and system design decisions based on an understanding of privacy risk and the options available for mitigating that risk.

Based on the results, it should be possible to create a consistent format and structured process for analyzing technical and legal compliance with relevant regulations and internal policies. This structured process provides a framework to ensure that privacy is considered in all IT projects, from the conceptual and requirements analysis stage to the final design approval, funding, implementation and communication stage, so that privacy compliance is built into projects rather than retrofitted.

The focus and extent of privacy impact analysis or assessment may vary

depending on changes in technology, processes or people as shown in **figure**

5.3.

Figure 5.3—Changes That Impact Privacy

Technology

Processes

People

• New programs

• Change management

• Business partners

• Changes in existing

• Business process reengineering

• Service providers

programs

• Enhanced accessibility rules

• Additional system

• New systems

linkages

• New operations

• Data warehouse

• Vendors

• New products

The IS auditor may also be called on to give assurance on compliance with privacy policy, laws and other regulations. To fulfill this role, the IS auditor should:

• Identify and understand compliance requirements regarding privacy from laws, regulations and contract agreements. Depending on the assignment, IS auditors may need to seek legal or expert opinion on these.

• Review management's privacy policy to ascertain whether it takes into

consideration the requirement of these privacy laws and regulations.

• Check whether personal sensitive data are correctly managed in respect to these requirements.

• Verify that the correct security measures are adopted.

5.2.1 AUDIT CONSIDERATIONS FOR PRIVACY

Privacy should also be considered when conducting an audit. The following seven categories of privacy should be considered when developing audit objectives:

1. Privacy of person

2. Privacy of behavior and action

3. Privacy of communication

4. Privacy of data and image (information)

5. Privacy of thoughts and feelings

6. Privacy of location and space (territorial)

7. Privacy of association

ISACA describes several privacy principles for audit objectives that can be used as framework to consider most privacy issues when planning an audit.

Sample assurance considerations that are based on these privacy principles include:

• **Choice and consent**—Does the enterprise ensure that appropriate consent has been obtained prior to the transfer of personal information to other jurisdictions?

• **Legitimate purpose specification and use limitation**—Does the enterprise specify the purpose(s) for which personal information is collected?

• **Personal information and sensitive information life cycle**—Does the enterprise retain personal information for only as long as necessary?

• **Accuracy and quality**—Does the enterprise implement practices and processes to ensure that personal information is accurate, complete and up to date?

• **Openness, transparency and notice**—Does the enterprise provide clear and easily accessible information about its privacy policies and practices?

• **Individual participation**—Does the enterprise provide data subjects a

process to access their personal information?

• **Accountability**—Does the enterprise assign roles, responsibility, accountability and authority for performing privacy processes?

• **Security safeguards**—Does the enterprise ensure that appropriate security safeguards are in place for all personal information?

• **Monitoring, measuring and reporting**—Does the enterprise report compliance with policies, standards and laws?

• **Preventing harm**—Does the enterprise establish processes to mitigate any personal harms that may occur to data subjects?

• **Third-party/vendor management**—Does the enterprise implement governance processes to ensure the appropriate protections and use of personal information that are transferred to third parties?

• **Breach management**—Has the enterprise established a documented policy and supporting procedure for identifying, escalating and reporting incidents?

• **Security and privacy by design**—Does the enterprise ensure executive support for the identification of personal information and privacy risk within enterprise events?

• **Free flow of information and legitimate restriction**—Does the enterprise follow the requirements of applicable data protection authorities for the transfer of personal information across country borders?

Note: The CISA exam does not test on specific privacy laws and standards because they vary by country.

5.3 PHYSICAL ACCESS AND ENVIRONMENTAL CONTROLS

Security of information assets requires logical, physical and environmental security. The IS auditor needs to evaluate these controls. In many organizations, these controls are designed and implemented by facility management and not by the information security manager or IT. Most IT

assets require a controlled environment, such as temperature, humidity and power. The IS auditor need to assess these controls to provide assurance.

The information security management function provides:

• Management direction, including policy creation, involvement in significant information security strategies, establishment of and adherence to an information security architecture, and alignment of information security strategies with business strategies

• Management oversight and execution of essential information security operations. The former focuses on routine operations that affect information security, including access control; user identity management; and configuration management of other security building blocks, including intrusion detection and penetration testing systems, antimalware, and other processes. The latter includes information security incident management and security forensics.

• Management of information security technologies used within the organization

Information security is concerned with protecting the confidentially, integrity and authenticity of assets. If accomplished, controls are implemented.

Controls may be **proactive**, meaning that they attempt to prevent an incident, or controls may be **reactive**, meaning that they allow the detection, containment

and recovery from an incident. Proactive controls are often called safeguards, and reactive controls are known as countermeasures. For example, a sign that warns a person about a dangerous condition is a safeguard, whereas a fire extinguisher or sprinkler system is a

countermeasure.

Every organization has some controls in place, and a risk assessment should document these controls and their effectiveness in mitigating risk. In some cases, the controls may be sufficient, whereas in others, the controls may need adjustment or replacement. An effective control is one that prevents, detects and/or contains an incident and enables recovery from an event.

It is common for an organization to have some situations the existing controls are not sufficient to adequately protect the organization. In most cases, this requires the adjustment of the current controls or the implementation of new controls. However, it may not be feasible to reduce the risk to an acceptable level by either adjusting or implementing controls due to reasons such as

cost, job requirements or availability of controls. An example of this is in a small organization when an individual is given administrator rights on a system and there is not adequate segregation of duties (SoD). In this case, it may not be feasible to implement a new or enhanced control; some personnel need administrator rights to perform their jobs, and the risk cannot justify the cost of hiring new staff to address SoD. In such instances, compensating controls may be considered to reduce the risk. Compensating controls address the weaknesses in the existing controls through concepts such as layered defense, increased supervision, procedural controls, or increased audits and logging of system activity. These measures will work to compensate for the risk that could not be addressed in other ways.

5.3.1 MANAGERIAL, TECHNICAL AND PHYSICAL

CONTROLS

Controls are often divided into three groups, as shown in **figure 5.4.**

Figure 5.4—Control Methods

Category

Description

Managerial (administrative)

Controls related to the oversight, reporting, procedures and operations of a process. These include policy, procedures, balancing, employee development and compliance reporting.

Technical

Controls also known as logical controls and are provided through the use of technology, piece of equipment or device. Examples include firewalls, network or host-based intrusion detection systems (IDSs), passwords, and antivirus software. A technical control requires proper managerial (administrative) controls to operate correctly.

Physical

Controls that are locks, fences, closed-circuit TV (CCTV), and

devices that are installed to physically restrict access to a facility or hardware. Physical controls require maintenance, monitoring and the ability to assess and react to an alert should a problem be indicated.

Further controls within these groups may be preventive, detective or corrective (see chapter 1, Information Systems Auditing Process, for more information). An example of a control matrix is shown in **figure 5.5**. Many controls may fit into more than one classification.

Figure 5.5—Control Matrix			
	Managerial	**Technical**	**Physical**
Preventive	User registration process	Login screen	Fence
Detective	Audit	Intrusion detection system (IDS)	Motion sensor
Corrective	Remove access	Network isolation	Close fire doors

5.3.2 CONTROL MONITORING AND EFFECTIVENESS

To support the ability to monitor and report on risk, the IS auditor should validate that processes, logs and audit hooks (red flags) have been placed into the control framework. This allows for the monitoring and evaluation of controls. As controls are designed, implemented and operated, the IS auditor should ensure that logs are enabled, controls are able to be tested and regular reporting procedures are developed.

The IS auditor should also ensure that the capability to monitor a control and to support monitoring systems is addressed in control design. If the organization is using a managed security service provider (MSSP) or a security information and event management (SIEM) system, the ability to capture data, and the notification to the operations staff on the deployment of the system, are necessary.

5.3.3 ENVIRONMENTAL EXPOSURES AND CONTROLS

As with any other manmade objects, IT infrastructure and information assets are exposed to the environment. The IS auditor should be aware of these exposures and the controls used to mitigate them.

Equipment Issues and Exposures Related to the Environment

Environmental exposures are due primarily to naturally occurring events such as lightning storms, earthquakes, volcanic eruptions, hurricanes, tornados and other types of extreme weather conditions. The result of such conditions can lead to many types of problems. One particular area of concern is power failures of computer and supporting environmental systems. Generally, power failures can be grouped into four distinct categories, based on the duration and relative severity of the failure:

• **Total failure (blackout)**—A complete loss of electrical power, which may span from a single building to an entire geographical area and is often caused by weather conditions (e.g., storm, earthquake) or the inability of an electrical utility company to meet user demands (e.g., during summer months)

• **Severely reduced voltage (brownout)**—The failure of an electrical utility company to supply power within an acceptable range (i.e., 108–125 volts AC in the US). Such failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

• **Sags, spikes and surges**—Temporary and rapid decreases (sags) or increases (spikes and surges) in voltage levels. These anomalies can cause loss of data, data corruption, network transmission errors or physical damage to hardware devices (e.g., hard disks or memory chips).

• **Electromagnetic interference (EMI)**—Caused by electrical storms or noisy electrical equipment (e.g., motors, fluorescent lighting, radio transmitters). This interference may cause computer systems to hang or crash as well as damages similar to those caused by sags, spikes and surges.

Short-term interruptions, such as sags, spikes and surges, which last from a few millionths to a few thousandths of a second, can be prevented by using properly placed surge protectors. Intermediate-term interruptions, which last from a few seconds to 30 minutes, can be controlled by uninterruptible power supply (UPS) devices. Finally, long-term interruptions, which last from a few hours to several days, require the use of alternate power generators. These generators may be portable devices or part of the building's infrastructure and are powered by alternative sources of energy such as diesel, gasoline or propane.

Another area of concern deals with water damage/flooding. This is a concern even with facilities located on upper floors of high-rise buildings because water

damage typically occurs from broken water pipes.

Manmade concerns include terrorist threats/attacks, vandalism, electrical shock and equipment failure.

Some questions that organizations must address related to environmental issues and exposures include the following:

• Is the power supply to the computer equipment properly controlled to ensure that power remains within the manufacturer's specifications?

• Are the air conditioning, humidity and ventilation control systems for the computer equipment adequate to maintain temperatures within

manufacturers' specifications?

• Is the computer equipment protected from the effects of static electricity, using an antistatic rug or antistatic spray?

• Is the computer equipment kept free of dust, smoke and other particulate matter such as food?

• Do policies exist that prohibit the consumption of food, beverage and tobacco products near computer equipment?

• Are backup media protected from damage due to temperature extremes, the effects of magnetic fields and water damage?

Controls for Environmental Exposures

Environmental exposures should be afforded the same level of protection as physical and logical exposures.

Alarm Control Panels

An alarm control panel should ideally be:

• Separated from burglar or security systems located on the premises

• Accessible to fire department personnel at all times

• Located in a weatherproof box

• In accordance with temperature requirements set by the manufacturer

• Situated in a controlled room to prevent access by unauthorized personnel

• Allocated power from a dedicated and separate circuit

• Able to control or disable separate zones within the facilities

• In adherence with local and national regulations and approved by local authorities

Water and Smoke Detectors

In the computer room, water detectors should be placed under raised floors and near drain holes, even if the computer room is on a high floor (because of possible water leaks). Any unattended equipment storage facilities should also have water detectors. When activated, the detectors should produce an audible alarm that can be heard by security and control personnel. The location of the water detectors should be marked on the raised computer room floor for easy identification and access. On hearing the alarm, specific individuals should be responsible for investigating the cause and initiating remedial action; other staff should be made aware by security and control personnel that there is a risk of electric shock.

Smoke detectors should be installed above and below the ceiling tiles throughout the facilities and below the raised computer room floor. The detectors should produce an audible alarm when activated and be linked to a monitored station (preferably by the fire department). The location of the smoke detectors above the ceiling tiles and below the raised floor should be marked on the tiling for easy identification and access. Smoke detectors should supplement, not replace, fire suppression systems.

Visual verification of the presence of water and smoke detectors in the computer room is needed. Whether the power supply to these detectors is sufficient should be determined, especially in instances of battery-operated devices. Also, the locations of the devices should be placed to give early warning of a fire, such as immediately above the computer equipment they are protecting and should be clearly marked and visible.

Handheld Fire Extinguishers

Fire extinguishers should be in strategic locations throughout the facility.

They should be tagged for inspection and inspected at least annually.

Manual Fire Alarms

Hand-pull fire alarms should be placed strategically throughout the facility.

These are normally located near exit doors to ensure personnel safety. The resulting audible alarm should be linked to a monitored guard station.

Fire Suppression Systems

These systems are designed to automatically activate immediately after detection of high heat, typically generated by fire. Like smoke detectors, the system should produce an audible alarm when activated and be linked to a central guard station that is regularly monitored. The system should also be inspected and tested annually. Testing intervals should comply with industry and insurance standards and guidelines. Ideally, the system should automatically trigger other mechanisms to localize the fire. This includes closing fire doors, notifying the fire department, closing off ventilation ducts and shutting down nonessential electrical equipment. In addition, the system should be segmented so a fire in one part of a large facility does not activate the entire system.

Broadly speaking, there are two methods for applying an extinguishing agent: total flooding and local application.

Systems working under a *total flooding* principle apply an extinguishing agent to a three-dimensional enclosed space in order to achieve a concentration of the agent (volume percent of the agent in air) adequate to extinguish the fire. These types of systems may be operated automatically by detection and related controls or manually by the operation of a system actuator. Systems working under a *local application* principle apply an extinguishing agent directly onto a fire (usually a two- dimensional area), or into the three-dimensional region immediately surrounding the substance or object on fire. The main difference between local application and total flooding designs is the absence of physical barriers enclosing the fire space in the local application design.

In the context of automatic extinguishing systems, local application does not normally refer to the use of manually operated wheeled or portable fire extinguishers, although the nature of the agent delivery is similar.

Typical fire suppression systems include, but are not limited to:

• **Water-based systems (sprinkler systems)**—Water is always present in the system piping, which can potentially leak, causing damage to equipment.

• **Dry-pipe sprinkling systems**—Water does not flow until the fire alarm activates a pump.

• **Halon systems**—Note: Halon was banned by the Montreal (Canada) Protocol of 1987. As a banned gas, all Halon installations are required by international agreements to be removed.

• **FM-200®, also called heptafluoropropane, HFC-227 or HFC-227ea (ISO name)**—This is often considered the preferred option for fire suppression.

• **Argonite® (a mixture of 50 percent argon [Ar] and 50 percent nitrogen [N2])**—Argonite is not recommended because it is harmful to human life.

• **Carbon dioxide systems**—Due to the threat to human life, it is illegal for these systems to be set to automatic release if any human may be in the area.

Fire suppression systems are expensive to test, and therefore, IS auditors may need to limit their tests to reviewing documentation to ensure that the system has been inspected and tested within the last year. The exact testing interval should comply with industry and insurance standards and guidelines.

Strategically Locating the Computer Room

To reduce the risk of flooding, the computer room should not be located in the basement or top floor. If located in a multistory building, studies show that the best location for the computer room—the location that reduces the risk of fire, smoke and water damage—is on the middle floors (e.g., third, fourth, fifth or sixth floor). Adjacent water or gas pipes should be avoided except in the case of fire suppression systems. Care should be taken to avoid locating computer rooms adjacent to areas where functions carrying a high risk are carried out, such as

paper storage. The activity of neighboring organizations should be considered when establishing a computer facility.

Locations adjacent to, or on the final path to, an airport or a chemical works where explosive gases may be present, for example, should be avoided.

If a data center is already located in an area vulnerable to flooding, such as a

basement, an alternative to costly removal is the provision of a plastic sheet, or umbrella, covering the area, which diverts any water flow away from the sensitive equipment.

Regular Inspection by Fire Department

To ensure that all fire detection systems comply with building codes, the fire department should inspect the system and facilities annually. Also, the fire department should be notified of the location of the computer room, so it can be prepared with equipment appropriate for electrical fires.

The IS auditor should contact the person responsible for fire equipment maintenance and asked if a local fire department inspector or insurance evaluator has been recently invited to tour and inspect the facilities. If so, a copy of the report should be obtained, and how to address the noted deficiencies should be determined.

Fireproof Walls, Floors and Ceilings of the Computer Room

Walls surrounding the information processing facility should contain or block fire from spreading. The surrounding walls should be from true floor to the true ceiling and should have at least a two-hour fire resistance rating.

With the assistance of building management, the documentation that identifies the fire rating of the walls surrounding the information processing facility (IPF) should be located. These walls should have at least a two-hour fire resistance rating.

Electrical Surge Protectors

These electrical devices reduce the risk of damage to equipment due to power spikes. Voltage regulators measure the incoming electrical current and either

increase or decrease the charge to ensure a consistent current. Such protectors are typically built into the UPS system.

Uninterruptible Power Supply/Generator

A UPS system consists of a battery or gasoline-powered generator that interfaces with the electrical power entering the facility and the electrical power entering the computer. The system typically cleanses the power to

ensure that voltage into the computer is consistent. The UPS continues providing electrical power from the generator to the computer for a defined length of time should a power failure occur. Depending on the sophistication of the UPS, electrical power could continue to flow for days or for just a few minutes to permit an orderly computer shutdown. A UPS system can be built into a computer or can be an external piece of equipment. The most recent test date should be determined, and the test reports should be reviewed.

Emergency Power-off Switch

There may be a need to immediately shut off power to the computer and peripheral devices, such as during a computer room fire or emergency evacuation. Two emergency power-off switches should serve this purpose—

one in the computer room, the other near, but outside, the computer room.

Switches should be clearly labeled and easily accessible, for this purpose, yet they should still be secure from unauthorized people. The switches should be shielded to prevent accidental activation. Furthermore, an IS auditor should assess the need to have them under video surveillance, as a dissuasive control against malicious insiders and a source of information for incident handling.

The presence of electrical surge protectors on sensitive and expensive computer equipment should be visually observed.

Power Leads From Two Substations

Electrical power lines that feed into the facility are exposed to many environmental hazards—water, fire, lightning, cutting due to careless digging, etc. To reduce the risk of a power failure due to these events that, for the most part, are beyond the control of the organization, redundant power lines should

feed into the facility. In this way, interruption of one power line does not adversely affect electrical supply.

With the assistance of building management, documentation concerning the use and placement of redundant power lines into the IPF should be located.

Fully Documented and Tested Business Continuity Plan

See section 4.15, Business Continuity Plan, for more information on business

continuity plans (BCPs).

Wiring Placed in Electrical Panels and Conduit

To reduce the risk of an electrical fire occurring and spreading, wiring should be placed in fire-resistant panels and conduit. This conduit generally lies under the fire-resistant raised computer room floor.

Inhibited Activities Within the Information Processing Facility

Food, drink and tobacco use can cause fires, the buildup of contaminants or damage to sensitive equipment (especially in the case of liquids). They should be prohibited from the IPF. This prohibition should be overt, such as with a sign on the entryway.

Fire-resistant Office Materials

Wastebaskets, curtains, desks, cabinets and other general office materials in the IPF should be fire-resistant. Cleaning fluids for desktops, console screens and other office furniture/fixtures should not be flammable.

Documented and Tested Emergency Evacuation Plans

Evacuation plans should emphasize human safety but should not leave IPFs physically unsecured. Procedures should be in place for a controlled shutdown of the computer in an emergency situation, if time permits.

A copy of the emergency evacuation plan should be obtained. It should be examined to determine whether it describes how to leave the IPFs in an organized manner that does not leave the facilities physically insecure. A sample

of IS employees should be interviewed to determine if they are familiar with the documented plan. The emergency evacuation plans should be posted throughout the facilities.

Humidity/Temperature Control

The IPF should be visited on regular intervals to determine whether temperature and humidity are adequate.

5.3.4 PHYSICAL ACCESS EXPOSURES AND CONTROLS

Physical exposures can result in financial loss, legal repercussions, loss of

credibility or loss of competitive edge. They primarily originate from natural and man-made hazards and can expose the business to unauthorized access and unavailability of the business information.

Physical Access Issues and Exposures

Physical access issues are a major concern in security. Exposures and possible perpetrators are described in the following subsections.

Physical Access Exposures

Exposures that exist from accidental or intentional violation of these access paths include:

• Unauthorized entry

• Damage, vandalism or theft to equipment or documents

• Copying or viewing of sensitive or copyrighted information

• Alteration of sensitive equipment and information

• Public disclosure of sensitive information

• Abuse of data processing resources

• Blackmail

• Embezzlement

• Wiretapping/eavesdropping

Possible perpetrators include employees with authorized or unauthorized access who are:

• Disgruntled (upset by or concerned about some action by the organization or its management)

• On strike

• Threatened by disciplinary action or dismissal

• Addicted to a substance or gambling

• Experiencing financial or emotional problems

• Notified of their termination

Other possible perpetrators could include:

• Former employees

• Interested or informed outsiders such as competitors, thieves, organized crime and hackers

• An accidental ignorant (e.g., someone who unknowingly perpetrates a

violation)

The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent.

Other questions and concerns to consider include the following:

• Are hardware facilities reasonably protected against forced entry?

• Are keys to the computer facilities adequately controlled to reduce the risk of unauthorized access?

• Are computer terminals locked or otherwise secured to prevent removal of boards, chips and the computer itself?

• Are authorized equipment passes required before computer equipment can be removed from its normal secure surroundings?

• From an IS perspective, facilities to be protected include:

– Programming area

– Computer room

– Operator consoles and terminals

– Tape library, tapes, disks and all magnetic media

– Storage rooms and supplies

– Offsite backup file storage facility

– Input/output control room

– Communications closets

– Telecommunications equipment (including radios, satellites, wiring, modems and external network connections)

– Microcomputers and PCs

– Power sources

– Disposal sites

– Minicomputer establishments

– Dedicated telephones/telephone lines

– Control units and front-end processors

– Portable equipment (handheld scanners and coding devices, bar code readers, laptop computers, printers, pocket local area network (LAN) adapters and

others)

– Onsite and remote printers

– Local area networks

Additionally, system, infrastructure or software application documentation should be protected against unauthorized access.

For these safeguards to be effective, they must extend beyond the computer facility to include any vulnerable access points within the entire organization and at organizational boundaries/interfaces with external organizations. This may include remote locations and rented, leased or shared facilities.

Additionally, the IS auditor may require assurances that similar controls exist within service providers or other third parties, if they are potentially vulnerable access points to sensitive information within the organization.

Physical Access Controls

Physical access controls are designed to protect the organization from unauthorized access. These controls should limit access to only those individuals authorized by management. This authorization may be explicit, as in a door lock for which management has authorized who has a key, or implicit, as in a job description that implies a need to access sensitive reports and documents.

Bolting door locks require the traditional metal key to gain entry. The key should be stamped “do not duplicate” and should be stored and issued under strict management control.

Combination door locks (cipher locks) use a numeric key pad or dial to gain entry and are often seen at airport gate entry doors and smaller server rooms. The combination should be changed at regular intervals or whenever an employee with access is transferred, fired or subject to disciplinary action.

This reduces the risk of the combination being known by unauthorized people.

Electronic door locks use a magnetic or embedded chip-based plastic card key or token entered into a sensor reader to gain access. A special code stored in the card or token is read by the sensor device that then activates the door locking

mechanism. Electronic door locks have the following advantages over bolting and combination locks:

• Through the special internal code, cards can be assigned to an identifiable

individual.

• Through the special internal code and sensor devices, access can be restricted based on the individual's unique access needs. Restrictions can be assigned to particular doors or to particular hours of the day.

• They are difficult to duplicate.

• Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen. Silent or audible alarms can be automatically activated if unauthorized entry is attempted. Issuing, accounting for and retrieving the card keys is an administrative process that should be carefully controlled. The card key is an important item to retrieve when an employee leaves the firm. An example of a common technique used for card entry is the swipe card. A swipe card is a physical control technique that uses a plastic card with a magnetic strip containing encoded data to provide access to restricted or secure locations. The encoded data can be read by a slotted electronic device. After a card has been swiped, the application attached to the slotted electronic device prevents unauthorized physical access to those sensitive locations, as well as logs all card users that try to gain access to the secure location.

Biometric door locks are activated by an individual's unique body features, such as voice, retina, fingerprint, hand geometry or signature. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

Manual logging means all visitors are required to sign a visitor's log indicating their name, the company they are representing, reason for visiting, person to see and date and time of entry and departure. Logging is typically done at the front reception desk and entrance to the computer room. Before gaining access, visitors should also be required to provide verification of identification such as a driver's license or vendor identification tag.

Electronic logging is a feature of electronic and biometric security systems.

All access can be logged, with unsuccessful attempts being highlighted.

Identification badges (photo IDs) should be worn and displayed by all personnel. Visitor badges should be a different color from employee badges

for easy identification. Sophisticated photo IDs can also be used as electronic card keys. Issuing, accounting for and retrieving the badges is an administrative process that must be carefully controlled.

Video cameras, including motion-activated models, should be located at strategic points and monitored by security guards. The video surveillance recording should be retained for possible future playback, and it should be recorded in sufficient resolution to permit enlarging the image to identify an intruder.

Security guards are very useful if supplemented by video cameras and locked doors. Guards supplied by an external agency should be bonded to protect the organization from loss.

Controlled visitor access means all visitors should be escorted by a responsible employee. Visitors include friends, maintenance personnel, computer vendors, consultants (unless long-term, in which case special guest access may be provided) and external auditors.

All service contract personnel, such as cleaning people and offsite storage services, should be **bonded personnel**. This does not improve physical security but limits the financial exposure of the organization.

Deadman doors, also referred to as a mantrap or airlock entrance, uses two doors and is typically found in entries to facilities, such as computer rooms and high-security areas. For the second door to operate, the first entry door must close and lock, with only one person permitted in the holding area. This reduces the risk of piggybacking, when an unauthorized person follows an authorized person through a secured entry. In some installations, this same effect is accomplished through the use of a full height turnstile. Deadman doors may also be used for delivery and dispatch areas where outer doors open to admit a truck and the inner doors cannot be opened to load or unload until the outer doors are closed and locked.

Computer workstation locks secure the device to the desk, prevent the

computer from being turned on or disengage keyboard recognition, thus preventing use. Another available feature is locks that prevent turning on a

PC workstation until a key lock is unlocked by a turnkey or card key. This is sometimes seen in the case of high-security workstations, such as those that process payroll.

A c**ontrolled single-entry point,** monitored by a receptionist, should be used by all incoming personnel. Multiple entry points increase the risk of unauthorized entry. Unnecessary or unused entry points, such as doors to outside smoking or break areas, should be eliminated. Emergency exits can be wired to an alarmed panic bar for quick evacuation.

An **alarm system** should be linked to inactive entry points, motion detectors, and the reverse flow of enter- or exit-only doors. Security personnel should be able to hear the alarm when activated.

Secured report/document distribution carts such as mail carts, should be covered and locked and should not be left unattended.

Facilities such as computer rooms should not be visible or identifiable from the outside; there should be no windows or directional signs. The building or department directory should discreetly identify only the general location of the information processing facility. If windows are present, they should be constructed of reinforced glass and, if on the ground floor of the building, further protected for example, by bars.

Auditing Physical Access

Touring the computer site is useful for the auditor to gain an overall understanding and perception of the installation being reviewed. As with environmental controls where the site is owned by a third party, a contractual right of audit may be required. This tour provides the opportunity to begin reviewing physical access restrictions (e.g., control over employees, visitors, intruders and vendors).

The computer site (i.e., computer room, developers' area, media storage, printer stations and management offices) and any offsite storage facilities should be included in this tour.

Much of the testing of physical safeguards can be achieved by visually

observing the previously noted safeguards. Documents to assist with this effort include emergency evacuation procedures, inspection tags (recent inspection?), fire suppression system test results (successful? recently tested?) and key lock logs (all keys accounted for and not outstanding to former employees or consultants?).

Testing should extend beyond the computer room to include the following related facilities:

• Location of all operator consoles

• Printer rooms

• Computer storage rooms (this includes equipment, paper and supply rooms)

• UPS/generator

• Location of all communications equipment identified on the network diagram

• Media storage

• Offsite backup storage facility

To complete a thorough test, the IS auditor should look above the ceiling panels and below the raised floor in the computer operations center, observing smoke and water detectors, general cleanliness, and walls that extend all the way to the real ceiling (not just the fake/suspended ceiling). For a ground-floor computer room, the auditor may also consider walking around the outside of the room, viewing the location of any windows, examining emergency exit doors for evidence that they are routinely used (such as the presence of cigarette stubs or litter) and examining the air conditioning units.

The auditor should also consider whether any additional threats exist close to the room, such as storage of dangerous or flammable material.

The following paths of physical entry should be evaluated for proper security:

• All entry doors

• Emergency exit doors

• Glass windows and walls

• Movable walls and modular cubicles

• Above suspended ceilings and beneath raised floors

• Ventilation systems

• Over a curtain, fake wall

5.4 IDENTITY AND ACCESS MANAGEMENT

Identification and authentication (I&A) is a critical building block of computer security because it is needed for most types of access control and is necessary for establishing user accountability. For most systems, I&A is the first line of defense because it prevents unauthorized access (or unauthorized processes) to a computer system or an information asset. Logical access can be implemented in various ways. The IS auditor should be aware of the strengths and weaknesses of various architectures as well as the risk associated with the different architectures and how they may be addressed.

Logical access controls are used to manage and protect information assets.

Logical security is often determined based on the job function of users. The success of logical access controls is tied to the strength of the authentication method. All user access to systems and data should be appropriately authorized and commensurate with the role of the individual. Authorization generally takes the form of signatures (physical or electronic) of relevant management. The strength of the authentication is proportional to the quality of the method used.

5.4.1 SYSTEM ACCESS PERMISSION

System access permission is the prerogative to act on a computer resource.

This usually refers to a technical privilege, such as the ability to read, create, modify or delete a file or data; execute a program; or open or use an external connection.

System access to computerized information resources is established, managed and controlled at the physical and/or logical level. Physical access controls restrict the entry and exit of personnel to an area such as an office building, suite, data center or room containing information processing equipment such as a LAN server. There are many types of physical access controls, including badges, memory cards, guard keys, true floor-to-ceiling wall construction fences, locks and biometrics. Logical system access controls restrict the logical resources of the system (transactions, data, programs, applications)

and are applied when the subject resource is needed. On the basis of identification and authentication of the user that requires a given resource and by analyzing the security profiles of the user and the resource, it is possible to determine if the requested access is to be allowed (i.e., the information that users can access, the programs or transactions that they can run, and the modifications that they can make). Such controls may be built into the operating system (OS), invoked through separate access control software and incorporated into application programs, database, network control devices and utilities (e.g., real-time performance monitors).

Physical or logical system access to any computerized information should be on a documented need-to-know basis (often referred to as role-based) where there is a legitimate business requirement based on least privilege. Other considerations for granting access are accountability (e.g., unique user ID) and traceability (e.g., logs). These principles should be used by IS auditors when they evaluate the appropriateness of criteria for defining permissions and granting security privileges. Organizations should establish such basic criteria for assigning technical access to specific data, programs, devices and resources, including who will have access and what level of access they will be allowed. For instance, it may be desirable for everyone in the organization to have access to specific information on the system such as the data displayed on an organization’s daily calendar of meetings. The program that formats and displays the calendar might be modifiable by only a few system administrators, while the OS controlling that program might be directly accessible by still fewer.

The IT assets under logical security can be grouped in four layers—networks, platforms, databases and applications. This concept of layered security for system access provides greater scope and granularity of control to information resources. For example, network and platform layers provide pervasive general systems control over users authenticating into systems, system software and

application configurations, data sets, load libraries, and any production data set libraries. Database and application controls generally provide a greater degree of control over user activity within a particular business process by controlling access to records, specific data fields and transactions.

The information owner or manager who is responsible for the accurate use and reporting of information should provide written authorization for users or defined roles to gain access to information resources under their control. The manager should hand over this documentation directly to the security administrator to ensure that mishandling or alteration of the authorization does not occur.

Logical access capabilities are implemented by security administration in a set of access rules that stipulate which users (or groups of users) are authorized to access a resource at a particular level (e.g., read-, update- or execute-only) and under which conditions (e.g., time of the day or a subset of computer terminals). The security administrator invokes the appropriate system access control mechanism upon receipt of a proper authorization request from the information owner or manager to grant a specified user the rights for access to, or use of, a protected resource. The IS auditor should be aware that access is granted to the organization's information systems using the principles of need-to-know, least privilege and SoD.

Reviews of access authorization should be evaluated regularly to ensure that they are still valid. Personnel and departmental changes, malicious efforts, and just plain carelessness result in authorization creep and can impact the effectiveness of access controls. Many times, access is not removed when personnel leave an organization, thus increasing the risk of unauthorized access. For this reason, the information asset owner should review access controls periodically with a predetermined authorization matrix that defines the least-privileged access level and authority for an individual/role with reference to his/her job roles and responsibilities. Any access exceeding the access philosophy in authorized matrix or in actual access levels granted on a system should be updated and changed accordingly. One of the good practices is to integrate the review of access rights with human resource processes. When an employee transfers to a different function (i.e., promotions, lateral transfers or demotions), access rights are adjusted at the same time. Development of a security-conscious culture increases the effectiveness of access controls.

Nonemployees with access to corporate IS resources should also be held

responsible for security compliance and be accountable for security breaches.

Nonemployees include contract employees, vendor programmers/analysts, maintenance personnel, clients, auditors, visitors and consultants. It should be understood that nonemployees are also accountable to the organization's security requirements.

5.4.2 MANDATORY AND DISCRETIONARY ACCESS CONTROLS

Mandatory access controls (MACs) are logical access control filters used to validate access credentials that cannot be controlled or modified by normal users or data owners; they act by default. Controls that may be configured or modified by the users or data owners are called discretionary access controls (DACs).

MACs are a good choice to enforce a ground level of critical security without possible exception, if this is required by corporate security policies or other security rules. A MAC could be carried out by comparing the sensitivity of the information resources, such as files, data or storage devices, kept on a user-unmodifiable tag attached to the security object with the security clearance of the accessing entity such as a user or an application. With MACs, only administrators may make decisions that are derived from policy.

Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy. MACs are prohibitive; anything that is not expressly permitted is forbidden.

DACs are a protection that may be activated or modified at the discretion of the data owner. This would be the case of data owner-defined sharing of information resources, where the data owner may select who will be enabled to access his/her resource and the security level of this access. DACs cannot override MACs; DACs act as an additional filter, prohibiting still more access with the same exclusionary principle.

When information systems enforce MAC policies, the systems must

distinguish between MAC and the discretionary policies that offer more

flexibility. This distinction must be ensured during object creation,

classification downgrading and labeling.

5.4.3 INFORMATION SECURITY AND EXTERNAL

PARTIES

The security of the organization's information and information processing facilities that are accessed, processed, communicated to or managed by external parties should be maintained and should not be reduced by the introduction of external party products or services. Any access to the organization's information processing facilities and processing and communication of information by external parties should be controlled.

Controls should be agreed to and defined in an agreement with the external party. Organizations shall gain the right to audit the implementation and operation of the resulting security controls. Such agreements can help reduce the risk associated with external parties.

Identification of Risk Related to External Parties

The risk to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access. If there is a need to allow an external party access to the information processing facilities or information of an organization, a risk assessment should be carried out to identify any requirements for specific controls. The identification of risk related to external party access should consider the issues depicted in **figure 5.6**.

Access by external parties to the organization's information should not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. Generally, all security requirements resulting from work with external parties or internal controls should be reflected by the agreement with the external party.

It should be ensured that the external party is aware of its obligations and accepts the responsibilities and liabilities involved in accessing, processing, communicating or managing the organization's information and information

processing facilities.

Figure 5.6—Risk Related to External Party Access

• The information processing facilities an external party is required to access

• The type of access the external party will have to the information and information processing facilities:

– Physical access (e.g., to offices, computer rooms and filing cabinets)

– Logical access (e.g., to an organization's databases and information systems)

– Network connectivity between the organization's and the external party's network(s) (e.g., permanent connection and remote access)

– Whether the access is taking place onsite or offsite

• The value and sensitivity of the information involved and its criticality for business operations

• The controls necessary to protect information that is not intended to be accessible by external parties

• The external party personnel involved in handling the organization's information

• How the organization or personnel authorized to have access can be identified, the authorization verified and how often this needs to be reconfirmed

• The different means and controls employed by the external party when storing, processing, communicating, sharing, exchanging and destroying information

• The impact of access not being available to the external party when required and the external party entering or receiving inaccurate or misleading information

• Practices and procedures to deal with information security incidents and potential damages and the terms and conditions for the continuation of external party access in the case of an information security incident

• Legal and regulatory requirements and other contractual obligations relevant to

the external party that should be taken into account

• How the interests of any other stakeholders may be affected by the arrangements External parties might put information at risk if their security management is inadequate. Controls should be identified and applied to administer external party access to information processing facilities. For example, if there is a special need for confidentiality of the information, nondisclosure agreements might be used. Organizations may face risk associated with

interorganizational processes, management and communication, if a high degree of outsourcing is applied or where there are several external parties involved.

Addressing Security When Dealing With Customers

All identified security requirements should be addressed before giving customers access to the organization's information or assets.

In addition to asset protection and access control policies, the items presented in **figure 5.7** should be considered to address security prior to giving customers access to any of the organization's assets (depending on the type

and extent of access given, not all of them may apply).

Figure 5.7—Customer Access Security Considerations

• Description of the product or service to be provided

• The different reasons, requirements and benefits for customer access

• Arrangements for reporting, notification and investigation of information inaccuracies (e.g., of personal details), information security incidents and security breaches

• The target level of service and unacceptable levels of service

• The right to monitor and revoke any activity related to the organization's assets

• The respective liabilities of the organization and the customer

• Responsibilities with respect to legal matters and ensuring that the legal requirements are met (e.g., data protection legislation), considering different national legal systems if the agreement involves cooperation with customers in other countries

• Intellectual property rights (IPRs), copyright assignment and protection of any collaborative work The security requirements related to customers accessing organizational assets can vary considerably depending on the information processing facilities and information being accessed. These security requirements can be addressed using customer agreements that contain all identified risk and security requirements.

Addressing Security in Third-party Agreements

Third-party agreements involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements. The agreement should ensure that there is no misunderstanding between the organization and the third party.

The organization should ensure that the agreement includes adequate indemnification provisions to protect against potential losses caused by the actions of the third party.

The contract terms that are listed in **figure 5.8** should be considered for inclusion in the agreement to satisfy the identified security requirements.

In general, it is very difficult to ensure the return or destruction of confidential information disclosed to a third party at the end of the agreement. To prevent unauthorized copies or use, printed documents should be consulted on site. Using technical controls, such as digital rights management (DRM) where access control technologies are used by

publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices, should be considered to set up the desired constraints such as the printing of the document, copying, authorized readers or using it after a certain date.

The agreements can vary considerably for different organizations and among the different types of third parties. Therefore, care should be taken to include all

identified risk and security requirements in the agreements. Where necessary, the required controls and procedures can be expanded in a security management plan.

If information security management is outsourced, the agreements should address how the third party will guarantee that adequate security, as defined by the risk assessment, will be maintained and how security will be adapted to identify and deal with changes to risk. Some of the differences between outsourcing and the other forms of third-party service provision include the question of liability, planning the transition period and potential disruption of operations during this period, contingency planning arrangements and due diligence reviews, and collection and management of information on security incidents. Therefore, it is important that the organization plans and manages the transition to an outsourced arrangement and has suitable processes in place to manage changes and the renegotiation/termination of agreements.

Figure 5.8—Recommended Contract Terms for Third-party Agreements

• Compliance with the organization’s information security policy by the third party

• Controls to ensure asset protection, including:

– Procedures to protect organizational assets, including information, software and hardware

– Any required physical protection controls and mechanisms

– Controls to ensure protection against malicious software

– Procedures to determine whether any compromise of the assets (e.g., loss or modification of information, software and hardware) has occurred

– Controls to ensure the return or destruction of information and assets at the end of or at an agreed point in time during the agreement

– Confidentiality, integrity, availability and any other relevant property of the assets

– Restrictions on copying and disclosing information, and using confidentiality

agreements

• User and administrator training in methods, procedures and security

• A means to ensure user awareness of information security responsibilities and issues

• Provision for the transfer of personnel, where appropriate

• Responsibilities regarding hardware and software installation and maintenance

• A clear reporting structure and agreed reporting formats

• A clear and specified process for change management

• Access control policy, covering:

– The different reasons, requirements and benefits that make the access by the third party necessary

– Permitted access methods and the control and use of unique identifiers such as user IDs and passwords

– An authorization process for user access and privileges

– A requirement to maintain a list of individuals authorized to use the services being made available and what their rights and privileges are with respect to such use

– A statement that all access that is not explicitly authorized is forbidden

– A process for revoking access rights or interrupting the connection between systems

• Arrangements for reporting, notification and investigation of information security incidents and security breaches as well as violations of the requirements stated in the agreement

• A description of the product or service to be provided and a description of the information to be made available along with its security classification

• The target level of service and unacceptable levels of service

• The definition of verifiable performance criteria, their monitoring and reporting

• The right to monitor and revoke any activity related to the organization’s assets

• The right to audit responsibilities defined in the agreement, to have those audits carried out by a third party and to enumerate the statutory rights of auditors (and, where appropriate, the provision of a service auditor’s report)

• The establishment of an escalation process for problem resolution

• Service continuity requirements, including measures for availability and reliability, in accordance with an organization’s business priorities

• The respective liabilities of the parties to the agreement

• Responsibilities with respect to legal matters and ensuring that the legal requirements are met (e.g., data protection legislation), considering different national legal systems if the agreement involves cooperation with organizations in other countries

• Intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work

• Involvement of the third party with subcontractors, and the security controls these subcontractors need to implement

• Conditions for renegotiation/termination of agreements such as:

– A contingency plan in case either party wishes to terminate the relationship before the end of the agreements

– A provision for renegotiation of agreements if the security requirements of the organization change

• Current documentation of asset lists, licenses, agreements or rights relating to them

• Non-assignability of the contract risk.

The procedures for continuing processing in the event that the third party becomes unable to supply its services need to be considered in the agreement to avoid any delay in arranging replacement services. Agreements with third parties may also involve other parties. Agreements granting third-party access should include allowance for designation of other eligible parties and conditions for their access and involvement. A requirement for the third party to have certified compliance with recognized security standards (e.g., ISO

27001) may need to be considered.

Generally, agreements are primarily developed by the organization. There may be occasions in some circumstances where an agreement may be developed and imposed upon an organization by a third party. The organization needs to ensure that its own security is not unnecessarily impacted by third-party requirements stipulated in imposed agreements.

Agreements with external parties may also involve other parties. Agreements granting an external party access should include an allowance for designation of other eligible parties and conditions for their access and involvement.

Human Resources Security and Third Parties

Proper information security practices should be in place to ensure that employees, contractors and third-party users understand their responsibilities and are suitable for their assigned roles. These practices can reduce the risk of theft, fraud or misuse of facilities. Specific security practices include:

• Security responsibilities should be addressed prior to employment in adequate job descriptions, and in terms and conditions of employment.

• All candidates for employment, contractors and third-party users should be adequately screened, especially for sensitive jobs.

• Employees, contractors and third-party users of information processing facilities should sign an agreement on their security roles and

responsibilities, including the need to maintain confidentiality.

Security roles and responsibilities of employees, contractors and third-party users should be defined and documented in accordance with the

organization’s information security policy.

Screening

All candidates for employment, contractors or third-party users should be subject to background verification checks. These should be carried out and documented in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed and the perceived risk. When using an agency to provide contractors, the contract with the agency should clearly specify the

agency’s responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern. In the same way, the agreement with the third party should clearly specify all responsibilities and notification procedures for screening.

Removal of Access Rights

The access rights of all employees, contractors and third-party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. The access rights that should be removed or adapted include physical and logical access, keys, identification cards, information processing facilities, subscriptions, and removal from any documentation that identifies them as a current member of the organization. This should include notifying partners and relevant third parties—if a departing employee has access to the third-party premises. If a departing employee, contractor or third-party user has known passwords for accounts remaining active, these should be changed upon termination or change of employment, contract or agreement. Access rights for information assets and information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors, such as:

• Whether the termination or change is initiated by the employee, contractor or third-party user, or by management and the reason of termination

• The current responsibilities of the employee, contractor or any other user

• The value of the assets currently accessible Procedures should be in place to ensure that information security management is promptly informed of all

employee movements, including employees leaving the organization.

5.4.4 LOGICAL ACCESS

Logical access is the ability to interact with computer resources granted using identification, authentication and authorization. Logical access controls are the primary means used to manage and protect information assets. They enact and substantiate management-designed policies and procedures intended to protect these assets and the controls are designed to reduce risk to a level acceptable to an organization. IS auditors need to understand this

relationship. In doing so, IS auditors should be able to analyze and evaluate the effectiveness of a logical access control in accomplishing information security objectives and avoiding losses resulting from exposures. These exposures can result in minor inconveniences to a total shutdown of computer functions.

Logical Access Exposures

Technical exposures are one type of exposure that exists due to accidental or intentional exploitation of logical access control weaknesses. Intentional exploitation of technical exposures might lead to computer crime. However, not all computer crimes exploit technical exposures. Technical exposures are the unauthorized activities interfering with normal processing, such as implementation or modification of data and software, locking or misusing user services, destroying data, compromising system usability, distracting processing resources, or spying data flow or users' activities at either the network, platform (OS), database or application level. Technical exposures include:

• **Data leakage**—Involves siphoning or leaking information out of the computer. This can involve dumping files to paper or can be as simple as stealing computer reports and tapes. Unlike product leakage, data leakage leaves the original copy, so it may go undetected.

• **Computer shutdown**—Initiated through terminals or personal computers connected directly (online) or remotely (via the Internet) to the computer.

Only individuals who know a high-level logon ID usually can initiate the shutdown process, but this security measure is effective only if proper security access controls are in place for the high-level logon ID and the telecommunications connections into the computer. Some systems have proven

to be vulnerable to shutting themselves down under certain conditions of overload.

Familiarization With the Enterprise's IT Environment

For IS auditors to effectively assess logical access controls within their organization, they first need to gain a technical and organizational understanding of the organization's IT environment. The purpose of this is to determine which areas from a risk standpoint warrant IS auditing attention in planning current and future work. This includes reviewing the network, OS

platform, database and application security layers associated with the organization's IT information systems architecture.

Paths of Logical Access

Access or points of entry to an organization's IS infrastructure can be gained through several avenues. Each avenue is subject to appropriate levels of access security.

A direct path of access (such as a PC terminal user tying directly into a mainframe) happens when the IS environment is under direct control of the main system and when the users are locally known individuals, with well-defined access profiles. Direct access related to a LAN is more complex, where many specific IS resources are tied to a common linking structure.

These resources may have different access paths/levels, normally mediated through LAN connectivity, and the network itself is considered an important IS resource at a higher access level.

A combination of direct, local network and remote access paths is the most common configuration. Complexity is increased by several intermediate devices that act as security doors among the various environments. The need of crossing low-security or totally open IT spaces, such as the Internet, also necessitates increased complexity. An example of an access path through common nodes is a back-end or front-end interconnected network of systems for internally or externally based users. Front-end systems are network-based systems connecting an organization to outside, untrusted networks, such as corporate websites, where a customer can access the website externally to initiate transactions that connect to a proxy server application which in turn connects to a back-end

database system to update a customer database. Front-end systems can also be internally based to automate business, paperless processes that tie into back-end systems in a similar manner.

General Points of Entry

General points of entry to either front- or back-end systems control the access from an organization's networking or telecommunications infrastructure into its information resources (e.g., applications, databases, facilities and networks). The approach followed is based on a client-server model. A large

organization can have thousands of interconnected network servers.

Connectivity in this environment needs to be controlled through a smaller set of primary domain controllers (servers), which enable a user to obtain access to specific secondary points of entry (e.g., application servers and databases).

General modes of access into this infrastructure occur through the following:

• **Network connectivity**—Access is gained by linking a PC to a segment of an organizations' network infrastructure, either through a physical or a wireless connection. At a minimum, such access requires user

identification and authentication to a domain-controlling server. More specific access to a particular application or database may also require the users to identify and authenticate themselves to that particular server (secondary point of entry). Other modes of access into the infrastructure can also occur through network management devices, such as routers and firewalls, which should be strictly controlled.

• **Remote access**—A user connects remotely to an organization's server, which generally requires the user to identify and authenticate him/herself to the server for access to specific functions that can be performed remotely (e.g., email, File Transfer Protocol [FTP] or some application-specific function). Complete access to view all network resources usually requires a virtual private network (VPN), which allows a secure authentication and connection into those resources where privileges have been granted.

Remote access points of entry can be extensive and should be centrally controlled where possible.

See section 5.5.7, Application of the OSI Model in Network

Architecture, for more information on VPN.

From a security standpoint, it is incumbent upon the organization to know all of the points of entry into its information resource infrastructure which, in many organizations, will not be a trivial task (e.g., thousands of remote access users). This is significant because any point of entry that is not appropriately controlled can potentially compromise the security of an organization's sensitive and critical information resources. When performing detailed network assessments and access control reviews, IS auditors should determine whether all points of entry are known and should support

management's effort in obtaining the resources to identify and manage all access paths.

5.4.5 ACCESS CONTROL SOFTWARE

IT has made it possible for computer systems to store and contain large quantities of sensitive data, increase the capability of sharing resources from one system to another and permit many users to access the system through Internet/intranet technologies. All of these factors have made organizations'

IS resources more widely and promptly accessible and available.

To protect an organization's information resources, access control software has become even more critical in assuring the confidentiality, integrity and availability of information resources. The purpose of access control software is to prevent the unauthorized access and modification to an organization's sensitive data and the use of system critical functions.

To achieve goal, it is necessary to apply access controls across all layers of an organization's IS architecture, including networks, platforms or OSs, databases, and application systems. Each of them usually features some form of I&A, access authorization, checking of specific information resources, and logging and reporting of user activities.

The greatest degree of protection in applying access control software against internal and external users' unauthorized access is at the network and platform/OS levels. These systems are also referred to as general support

systems, and they make up the primary infrastructure on which applications and database systems will reside.

OS access control software is typically restricted to privilege users and interfaces with network access control software and resides on network layer devices (e.g., routers and firewalls) that manage and control external access to organizations' networks. Additionally, OS access control software interfaces with database and/or application systems access controls to protect system libraries and user data sets.

General operating and/or application systems access control functions

include:

• Create or change user profiles.

• Assign user identification and authentication.

• Apply user logon limitation rules.

• Ensure users' access is commensurate with their job responsibilities.

• Ensure notification concerning proper use and access prior to initial login.

• Create individual accountability and auditability by logging user activities.

• Establish rules for access to specific information resources (e.g., system-level application resources and data).

• Log events.

• Report capabilities.

Database and/or application-level access control functions include the following:

• Create or change data files and database profiles

• Verify user authorization at the application and transaction level

• Verify user authorization within the application

• Verify user authorization at the field level for changes within a database

• Verify subsystem authorization for the user at the file level

• Log database/data communications access activities for monitoring access violations In summary, access control software is provided at different levels within an IS architecture, where each level provides a certain degree of security. Properties of such relationships are that upper layers (applications and databases) are dependent on lower, infrastructure-type layers to protect general system resources. Upper layers provide the granularity needed at the application level in segregating duties by function.

Figure 5.9 identifies the major gaps and corresponding best practices/recommendations. These have been segregated based on the key stages of identity and access management (IAM) in an organization.

5.4.6 IDENTIFICATION AND AUTHENTICATION

I&A is a critical building block of computer security because it is needed for most types of access control and is necessary for establishing user accountability. User accountability requires the linking of activities on a

computer system to specific individuals and, therefore, requires the system to identify users. For most systems, I&A is the first line of defense because it prevents unauthorized people (or unauthorized processes) from entering a computer system or accessing an information asset. If users are not properly identified and authenticated, particularly in today's open-system–networked environments, organizations have a higher exposure to risk of unauthorized access.

Figure 5.9—Key Concepts With Corresponding Security Concerns, Good Practices and Recommendations to Help Remediate the Gaps

Key Concepts of IAM

Identified Gaps and Security

Good

Concerns

Practices/Recommendations

Identify creation and access

Authorized approval not in place

The user's manager, the

request

resource owner or the

security officer, as necessary,

should authorize the user for

access to be granted.

Privileged access granted without

To justify its need, privileged

analyzing the need

access is to be provided after

two levels of approval-the

reporting manager and the

reporting manager's manager

or application, database or

server owner.

Group shared access

To justify its need, group

shared access is to be

provided after two levels of approval-the reporting manager and the reporting manager or application, database or server owner.

Utilize the principle of least privilege (i.e., just enough access should be given as needed).

Limit the servers on which the account can exist.

Ensure and preapprove the list of users who would be sharing the account.

Account owners should maintain and publish a list of users who have access to the shared account.

Validate the logging activities for shared accounts.

Passwords should be
changed on a regular basis.
The frequency should be
defined in the process
document.
If it is found that someone
obtains unauthorized access,
the password must be change
immediately.
Transfer request
Authorized approval not in place
The user's manager or the
resource owner or security
officer, as necessary, should
authorized access.
Access termination request
User IDs not revoked
At minimum, access
immediately after termination
termination should be done
in one working day (at

maximum, five working

days).

Password communication

Unsecure means to communicate

Passwords can be

passwords

communicated via user email

in encrypted format.

Passwords must be stored in

a sealed envelope.

Password management

Password parameters not

The password should be a

followed

minimum of eight characters

in length.

Password complexity not met

Passwords should contain a

Nonexistent password policies,

mix of lower- and uppercase

standards and guidelines

letters, numbers and

punctuation. Passwords

Use of shared passwords should be difficult to guess. The following should not be used:

- Words found in the dictionary
- Derivatives of the user ID
- Common character sequences
- Personal details, such as first name, last name, birth date, etc.

An encrypted history file should be maintained and should, at a minimum, retain the last 13 passwords for each user ID. Educate and make users aware of password confidentiality to hinder displaying and printing of passwords.

Password changes should be enforced: 30 days for privileged access IDs and 90 days for regular access.

At first login, a mandatory password change should be enforced.

At a minimum, five consecutive unsuccessful attempts should lead to suspension of the account until it is reset by the system administrator.

A time-out feature or Screensaver should be enabled after 15 minutes of inactivity.

Passwords must always be encrypted when held in storage for any significant period of time or when

transmitted over networks.

The password must be changed promptly when disclosure is suspected.

Each user ID should be uniquely identifiable, preferably to the username.

The last login date and time should be displayed for the user at the time of login

Policy administration

Lack of documented processes,

Document review should be policies and procedures done on regular basis- preferably yearly. The document must have:

Lack of timely process review

• The next review date

• The name of the owner of the process

• The name of the process approver

• The scope of the process

• Roles and responsibilities

• Measurements (key performance indicators)

• Workflows

• Templates, forms and formats

Validation

Validation process not in place/not adhered to

Each user account should be reevaluated by the user's manager at a fixed frequency-preferably six months for normal user accounts and three months

Timely action not taken for accounts that are not validated in the process

for privileged user accounts.

Validations should be

reviewed by the user's

manager or the resource,

application or data owner.

Reinstatement

Reinstatement without valid

All requests should be

authorization

checked for valid, granted

approvals. Lack of

approvals/incorrect

authorization requests should

be reinstated.

Authorization subprocess

Access given without

All requests should be

authorization

checked for valid granted

approvals. Lack of

approvals/incorrect

authorization requests should be blocked at the access request stage.

The user's manager, the resource owner or the security officer, as necessary, should authorize the user for access to be granted

SoD

Lack of SoD

All requests passing through the 1AM process should be validated for SoD policy checking. Requests that fail the SoD check should be blocked at the access request stage.

Log management

Lack of logging, auditing and reviewing of events

A log management process

should be in place.

Privileged access

Access provided to users without

To justify its need, privileged

validating the needs of access

access is to be provided after

two levels of approval-the

reporting manager and the

reporting manager's manager

or application, database or

server owner.

Periodic revalidation process not

Documented processes must

in place

be in place.

Revalidation of privilege

accounts must be conducted

on a quarterly basis.

Revalidation process in place

At a minimum, nonvalidated

although the nonvalidated

accounts should be

accounts are not terminated

terminated/locked in one

working day (at maximum,

five working days)

Dormant/orphan user accounts

Owners or custodians not

All accounts without an

identified for user accounts

owner or custodian need to

be identified and highlighted

so that they can be assigned

or removed.

Source: Kaur, Harmeet; “Identity and Access Management—Its Role in Sarbanes-Oxley Compliance,”

ISACA Journal Online, 2011, *www.isaca.org/Journal/archives/2011/Volume-6/Pages/JOnline-Identity-*

and-Access-Management-Its-Role-in-Sarbanes-Oxley-Compliance.aspx

Some of I&A’s more common vulnerabilities that may be exploited to gain unauthorized system access include:

• Weak authentication methods (e.g., no enforcement of password minimum length, complexity and change frequency)

• Use of simple or easily guessed passwords

• The potential for users to bypass the authentication mechanism

• The lack of confidentiality and integrity for the stored authentication information

• The lack of encryption for authentication and protection of information transmitted over a network

• The user’s lack of knowledge on the risk associated with sharing authentication elements (e.g., passwords and security tokens)

Authentication is typically categorized as something you know (e.g., password), something you have (e.g., token card) and something you are (or do) (a biometric feature). These techniques can be used independently or in combination to authenticate and identify a user. For example, a single-factor technique (something you know) involves the use of the traditional logon ID

and password. Something you know, such as a personal identification number (PIN), combined and associated with something you have, such as a token card, is known as a two-factor authentication technique. Something you are is a biometric authentication technique, such as a palm or iris biometric scan.

Each of these techniques is described in detail in the following sections.

A combination of more than one method, such as token and password, is referred to as multifactor authentication.

I&A are separate systems. They differ in respect to:

• Meaning

• Methods, peripherals and techniques supporting them

• Requirements in terms of secrecy and management

• Attributes—authentication does not have attributes in itself, while an identity may have a defined validity in time and other information attached to it.

Another key difference is that identity does not normally change, but authentication tokens must be regularly replaced to preserve their reliability

5.4.7 LOGON IDS AND PASSWORDS

Logon IDs and passwords are the components of a user identification and

authentication process, where the authentication is based on something you know. The computer can maintain an internal list of valid logon IDs and a corresponding set of access rules for each logon ID. These access rules are related to the computer resources. As a minimum requirement, access rules are usually specified at the OS level (controlling access to files) or within individual application systems (controlling access to menu functions and types of data or transactions).

The logon ID should be restricted to provide individual, but not group identification. If a group of users is to be formed for interchangeability, the system usually offers the ability to attach a logon ID to a named group, with common rights. Each user gets a unique logon ID that can be identified by the system. The format of logon IDs is typically standardized.

Features of Passwords

A password provides individual authentication. It should be easy for the user to remember but difficult for an intruder to determine.

Initial passwords may be allocated by the security administrator or generated by the system itself. When the user logs on for the first time, the system should force a password change to improve confidentiality. Initial password assignments should be randomly generated. The ID and password should be communicated in a controlled manner to ensure that only the appropriate user receives this information. New accounts without an initial password assignment should be suspended.

If the wrong password is entered a predefined number of times, the logon ID

should be automatically locked out. Locking-out may be made permanent (only the administrator may unlock the ID) or temporary (the system automatically unlocks the ID after a system-specified time period).

Users who have forgotten their password must notify a security administrator

—the only person with sufficient privileges to reset the password and/or unlock

the logon ID. The security administrator should reactivate the logon ID only after verifying the user's identification (challenge/response system).

To verify, the security administrator should return the user's call after

verifying his/her extension or calling his/her supervisor for verification.

Passwords should be hashed (a type of one-way encryption) and stored using a sufficiently strong algorithm. This allows checking passwords without the need of recording them explicitly. To reduce the risk of an intruder gaining access to other users' logon IDs, passwords should not be displayed in any form. Passwords are normally masked on a computer screen, and they are not shown on computer reports. Passwords should not be kept on index or card files or written on pieces of paper taped somewhere near the computer or inside a person's desk.

Passwords should be changed on a regular basis (e.g., every 30 days). The frequency depends on many factors including the criticality of the information access level, the nature of the organization, the IS architecture and technologies used. Passwords should be changed by the user at his/her computer, rather than by the administrator or in any location where their new password might be observed. The best method is to force the change by notifying the user prior to the password expiration date. The risk of allowing voluntary password changes is that users will not change their passwords unless forced to do so. Password management is stronger if a history of previously used passwords is maintained by the system and their reuse prohibited for a period, such as no reuse of the last 12 passwords.

A password for a logon ID should only be known by the individual user; if a password is known to more than one person, the accountability of the user for all activity within the account cannot be enforced.

Special treatment should be applied to supervisor or administrator accounts.

These accounts frequently allow full access to the system. Normally there are a limited number of such accounts per system/authentication level. For accountability, the administrator password should be known only by one individual. On the other hand, the organization should be able to access the system in an emergency situation when the administrator is not available. To enable this, practices, such as keeping the administrator password in a sealed

envelope, kept in a locked cabinet and available only to top managers should be implemented. This is sometimes referred to as a firecall ID.

All of the previous guidelines should be formalized in a password policy, and reading and acknowledging the policy should be mandatory. An acceptable use policy should also include the requirement to follow the policy.

Login ID and Password Good Practices

Logon ID requirements include the following:

• Logon ID syntax should follow an internal naming rule; however, this rule should be kept as confidential as the IDs themselves.

• Default system accounts—such as Guest, Administrator and Admin—

should be renamed or disabled whenever technically possible.

• Logon IDs not used after a predetermined period of time should be deactivated to prevent possible misuse. This can be done automatically by the system or manually by the security administrator.

• The system should automatically disconnect or lock a logon session if no activity has occurred for a period of time. This reduces the risk of misuse of an active logon session left unattended, because the user went to lunch, left for home, went to a meeting or otherwise forgot to log off. This is often referred to as a session time out. Regaining access should require the reentry of the authentication method, password, token, etc.

Password syntax rules include the following:

• Ideally, passwords should be a minimum of eight characters in length. The length of the password will, at times, depend on the sensitivity of the systems and data to be protected and the capability of the system being used. A passphrase is generally accepted as a more secure password.

• Passwords should require a combination of at least three of the following characteristics: alphanumeric, upper- and lower-case letters and special characters.

• Passwords should not be particularly identifiable with the user (such as first name, last name, spouse name, pet's name, etc.). Some organizations prohibit the use of vowels, making word association/guessing of passwords more difficult.

• The system should enforce regular password changes every 30 days and not permit previous password(s) to be used for at least a year after being changed.

At a minimum, these rules should be applied to individuals with privileged system account authority (e.g., system administrators, security

administrators) versus general users. Users with privileged authority need such access in establishing and managing appropriate system configurations.

However, such privileges enable the user to bypass any access control software restrictions that may exist on the system. The general rule to apply is that, the greater the degree of sensitivity of the access rights, the stricter the access controls should be.

Token Devices, One-time Passwords

In a common two-factor authentication technique, the user is assigned a microprocessor-controlled smart card, USB key or mobile device application synchronized with a specific authentication device on the system. This smart card/key/app is set to generate unique, time-dependent, pseudo-random strings that are called session passwords and are recognized by the authenticating device and program. They attest that the user is currently in possession of his/her own smart device. Each string is valid for only one logon session. Users must either physically read out and retype the string or insert the smart card/USB key in a reader/USB slot and type in their own memorized password to gain access to the system. This technique involves something you have (a device subject to theft) and something you know (a personal identification number).

5.4.8 BIOMETRICS

Biometric access controls are the best means of authenticating a user's identity based on a unique, measurable attribute or trait for verifying the identity of a human being. This control restricts computer access based on a physical or behavioral characteristic of the user. Due to advances in hardware efficiencies and storage, biometric systems are becoming a more viable option as an access control mechanism.

Using a biometric generally involves use of a reader device that interprets the individual's biometric features before permitting authorized access. However, this is not a flawless process because certain biometric features can change (e.g., scarred fingerprints, signature irregularities and change in voice). For this reason, biometric access control systems are not all equally effective and

easy to use. Entering a user's biometric into a system occurs through an enrollment process by storing a user's particular biometric feature.

This occurs through an iterative averaging process of acquiring a physical or behavioral sample, extracting unique data from the sample (converted into a mathematical code), creating an initial template, comparing new sample(s) with what has been stored and developing a final template that can be used to authenticate the user. Subsequent samples will be used in determining whether a match or non-match condition exists for granting access.

Three percentage-based quantitative measures are used to determine the performance of biometric control devices. One measure, the false-rejection rate (FRR), or type-I error rate, is the number of times an individual granted authority to use the system is falsely rejected by the system. An aggregate measure of type-I error rates is the failure-to-enroll rate (FER), the proportion of people who fail to be enrolled successfully. The other, referred to as the false-acceptance rate (FAR), or type-II error rate, is the number of times an individual not granted authority to use a system is falsely accepted by the system. Each biometric system may be adjusted to lower FRR or FAR, but as a general rule when one decreases, the other increases (and vice versa), and there is an adjustment point where the two errors are equal. An overall metric related to the two error types is the equal error rate (EER), which is the percent showing when false rejection and acceptance are equal. The lower the overall measure the more effective the biometric.

Physically Oriented Biometrics

Generally, the ordering of biometric devices with the best response times and lowest EERs are palm, hand, iris, retina, fingerprint and voice, respectively.

Palm-based biometric devices analyze physical characteristics associated with the palm such as ridges and valleys. This biometric involves placing the hand on a scanner where physical characteristics are captured.

As one of the oldest biometric techniques, **hand geometry** measures the physical characteristics of the users' hands and fingers from a three-dimensional perspective. The user places his hand, palm-down, on a metal

surface with five guidance pegs to ensure that fingers are placed properly and in the correct hand position. The template is built from measurements of physical geometric characteristics of a person's hand (usually 90

measurements)—for example, length, width, thickness and surface area.

Advantages of these systems are the social acceptance that they have received as well as the very little computer storage space that is required for the template, generally 10 to 20 bytes. The main disadvantage compared to other biometrics methods is the lack of uniqueness of hand geometry data.

Moreover, an injury to the hand may cause the measurements to change, resulting in recognition problems.

An **iris**, which has patterns associated with the colored portions surrounding the pupils, is unique for every individual and, therefore, a viable method for user identification. To capture this information, the user is asked to center his/her eye onto a device by seeing the reflection of their iris in the device.

After it is aligned, a camera takes a picture of the user's iris and compares it with a stored image. The iris is stable over time, having over 400

characteristics, although only approximately 260 of these are used to generate the template. As is the case with fingerprint scanning, the template carries less information than a high-quality image.

The key advantage to iris identification is that contact with the device is not needed, which contrasts with other forms of identification, such as fingerprint and retinal scans. Disadvantages of iris recognition are the high cost of the system, as compared to other biometric technologies, and the high amount of storage requirements needed to uniquely identify a user.

Retina scan uses optical technology to map the capillary pattern of the eye's retina. The user has to put his eye within 0.4 to 0.8 inches (1–2 cm) of the reader while an image of the pupil is taken. The patterns of the retina are measured at over 400 points to generate a 96-byte template. Retinal scan is extremely

reliable, and it has the lowest FAR among the current biometric methods. Disadvantages of retinal scanning include the need for fairly close physical contact with the scanning device, which impairs user acceptance, and the high cost.

Fingerprint access control is commonly used; the user places his/her finger on an optical device or silicon surface to get his/her fingerprint scanned. The template generated for the fingerprint, named “minutiae,” measures bifurcations, divergences, enclosures, endings and valleys in the ridge pattern. It contains only specific data about the fingerprint (the minutiae), not the whole image of the fingerprint itself. Additionally, the full fingerprint cannot be reconstructed from the template. Depending on the provider, the fingerprint template may use between 250 bytes to more than 1,000 bytes.

More storage space implies lower error rates. Fingerprint characteristics are described by a set of numeric values. While the user puts the finger in place for between two and three seconds, a typical image containing between 30

and 40 finger details is obtained and an automated comparison to the user’s template takes place.

Advantages of fingerprint scanning are low cost, small size of the device, ability to physically interface into existing client-server–based systems and ease of integration into existing access control methods. Disadvantages include the need for physical contact with the device and the possibility of poor-quality images due to residues, such as dirt and body oils, on the finger.

Additionally, fingerprint biometrics are not as effective as other techniques.

In **face-recognition biometric** devices, the biometric reader processes an image captured by a video camera, which is usually within 24 inches (60 cm) of the human face, isolating it from the other objects captured within the image. The reader analyzes images captured for general facial characteristics.

The template created is based on either generating two- or three-dimensional mapping arrays or by combining facial-metric measurements of the distance between specific facial features, such as the eyes, nose and mouth. Some vendors also include thermal imaging in the template. The face is considered to be one of the most natural and most “friendly” biometrics, and it is acceptable to users because it is fast and easy to use. The main disadvantage of face

recognition is the lack of uniqueness, which means that people who look alike may fool the device. Moreover, some systems cannot maintain high levels of performance as the database grows in size.

Behavior-oriented Biometrics

In **signature recognition**, also referred to as signature dynamics, the information from the reader is used to analyze two different areas of an individual's signature: the specific features of the signature and the specific features of the signing process. It includes speed, pen pressure, directions, stroke length and the points in time when the pen is lifted from the paper.

Advantages of this method are that it is fast, easy to use and has a low implementation cost. Other advantages are that even though a person might be able to duplicate the visual image of someone else's signature, it is difficult if not impossible to duplicate the dynamics (e.g., time duration in signing, pen-pressure, how often pen leaves signing block, etc.).

The main disadvantage is capturing the uniqueness of a signature particularly when a user does not sign their name in a consistent manner. For example, this may occur due to illness/disease or use of initials versus a complete signature. Additionally, users' signing behavior may change when signing onto signature identification and authentication "tablets" versus writing the signature in ink onto a piece of paper.

Voice recognition involves taking the acoustic signal of a person's voice, saying a "passphrase," and converting it to a unique digital code that can then be stored in a template (approximately 1,500 to 3,000 bytes). Voice recognition incorporates several variables or parameters to recognize one's voice/speech pattern including pitch, dynamics and waveform.

The main attraction of this method is that it can be used for telephone applications, where it can be deployed with no additional user hardware costs. It also has a high rate of acceptance among users.

Disadvantages of this method include the following:

• The large volume of storage requirements

• Changes to people's voices

• The possibility of misspoken phrases

• A clandestine recording of the user’s voice saying the passphrase could be made and played back to gain access.

• Background noises can interfere with the system.

Management of Biometrics

Management of biometrics should address effective security for the collection, distribution and processing of biometric data, encompassing:

• Data integrity, authenticity and nonrepudiation

• Management of biometric data across its life cycle—comprised of the enrollment, transmission, storage, verification, identification and termination processes

• Use of biometric technology, including one-to-one and one-to-many matching, for the identification and authentication of its users

• Application of biometric technology for internal and external, as well as logical and physical, access control

• Encapsulation of biometric data

• Techniques for the secure transmission and storage of biometric data

• Security of the physical hardware used throughout the biometric data life cycle

• Techniques for integrity and privacy protection of biometric data Management should develop and approve a biometric information

management and security (BIMS) policy. The auditor should use the BIMS

policy to gain a better understanding of the biometric systems in use. With respect to testing, the auditor should make sure this policy has been developed and the biometric information is being secured appropriately.

With any critical information system, logical and physical controls, including BCPs, should address this area.

Life cycle controls for the development of biometric solutions should be in place to cover the enrollment request, the template creation and storage, and the verification and identification procedures. The identification and authentication procedures for individual enrollment and template creation should be specified in the BIMS policy. Management needs to have controls in place to ensure that these procedures are being followed in accordance with this policy. If the biometric device malfunctions or is inoperable, backup authentication methods should also be developed. Controls should also be in place to protect the sample data as well as the template from modification during transmission.

5.4.9 SINGLE SIGN-ON

Users normally require access to a number of resources during the course of their daily routine. For example, users would first log into an OS and thereafter into various applications. For each OS application or other resource in use, users are required to provide a separate set of credentials to gain access. This can result in a situation where users' ability to remember passwords is significantly reduced. This also increases the chance that users will write them down on or near their workstation or area of work, thereby increasing the risk of a security breach within the organization. To address this situation, the concept of single sign-on (SSO) was developed. SSO is defined as the process for consolidating all organization platform-based administration, authentication and authorization functions into a single centralized administrative function. This function would provide the appropriate interfaces to the organization's information resources, which may include:

• Client-server and distributed systems

• Mainframe systems

• Network security including remote access mechanisms

The SSO process begins with the first instance where the user credentials are introduced into the organization's IT computing environment. The information resource or SSO server handling this function is referred to as the primary domain. Every other information resource, application or platform that uses those credentials is called a secondary domain.

The challenges in managing diverse platforms through SSO principally involve overcoming the heterogeneous nature of diverse networks, platforms, databases

and applications often found in organizations when establishing a set of credentials acceptable to all of these information resources. To effectively integrate into the SSO process, SSO administrators need to obtain an understanding of how each system manages credentialing information, access control list (ACL) authorization rules, and audit logs and reports.

Requirements developed in this regard should be based on security domain policies and procedures.

SSO advantages include:

• Multiple passwords are no longer required; therefore, a user may be more inclined and motivated to select a stronger password.

• It improves an administrator's ability to manage users' accounts and authorizations to all associated systems.

• It reduces administrative overhead in resetting forgotten passwords over multiple platforms and applications.

• It reduces the time taken by users to log into multiple applications and platforms.

SSO disadvantages include:

• Support for all major OS environments is difficult. SSO implementations will often require a number of solutions integrated into a total solution for an enterprise's IT architecture.

• The costs associated with SSO development can be significant when considering the nature and extent of interface development and

maintenance that may be necessary.

• The centralized nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information assets. For this reason, strong authentication in the form of complex password requirements and the use of biometrics is frequently implemented.

One example of SSO is Kerberos. Created by the Massachusetts Institute of

Technology, it is an authentication service used to validate services and users in a distributed computing environment (DCE). The role of the authentication service is to allow principals to positively identify themselves and participate in a DCE. Both users and servers authenticate themselves in a DCE

environment, unlike security in most other client-server systems where only users are authenticated. There are two distinct steps to authentication. At initial logon time, the Kerberos third-party protocol is used within DCE to verify the identity of a client requesting to participate in a DCE network. This process results in the client obtaining credentials initially registered with the trusted third party and cryptographically protected. These credentials form the basis for setting up secure sessions with DCE servers when the user tries to access resources.

SSO can also be addressed using the Security Assertion Markup Language

(SAML). This is open standard data format using XML to exchange authentication and authorization information between services. The single most important requirement that SAML addresses is web browser SSO.

5.4.10 AUTHORIZATION ISSUES

The authorization process used for access control requires that the system be able to identify and differentiate among users.

Access rules (authorization) specify who can access what. For example, access control is often based on least privilege, which refers to the granting to users of only those accesses required to perform their duties. Access should be on a documented need-to-know and need-to-do basis by type of access.

Computer access can be set for various levels (i.e., files, tables, data items).

When IS auditors review computer accessibility, they need to know what can be done with the access and what is restricted. For example, access restrictions at the file level generally include the following:

• Read, inquiry or copy only

• Write, create, update or delete only

• Execute only

• A combination of the above

The least dangerous type of access is read only, as long as the information being accessed is not sensitive or confidential. This is because the user cannot alter or use the computerized file beyond basic viewing or printing.

Access Control Lists

To provide security authorizations for the files and facilities listed previously, logical access control mechanisms use access authorization tables, also referred to as access control lists (ACLs) or access control tables. ACLs refer to a register of:

• Users (including groups, machines and processes) who have permission to use a particular system resource

• The types of access permitted

ACLs vary considerably in their capability and flexibility. Some only allow

specifications for certain preset groups (e.g., owner, group and world), while more advanced ACLs allow much more flexibility, such as user-defined groups. Also, more advanced ACLs can be used to explicitly deny access to a particular individual or group. With more advanced ACLs, access can be at the discretion of the policy maker (and implemented by the security administrator) or individual user, depending upon how the controls are technically implemented. When users changes job roles within an

organization, often their old access rights are not removed before adding their new required accesses. Without removing the old access rights, there could be a potential SoD issue.

Logical Access Security Administration

In a client-server environment, the access I&A and authorization process can be administered either through a centralized or decentralized environment.

The advantages of conducting security in a decentralized environment are:

• The security administration is onsite at the distributed location.

• Security issues are resolved in a timely manner.

• Security controls are monitored on a more frequent basis.

The risk associated with distributed responsibility for security administration includes:

• Local standards might be implemented rather than those required by the organization.

• Levels of security management might be below what can be maintained by a central administration.

• Management checks and audits that are often provided by central administration to ensure that standards are maintained might be

unavailable.

There are many ways to control remote and distributed sites:

• Software controls over access to the computer, data files and remote access to the network should be implemented.

• The physical control environment should be as secure as possible, with additions, such as lockable terminals and a locked computer room.

• Access from remote locations via modems and laptops to other

microcomputers should be controlled appropriately.

• Opportunities for unauthorized people to gain knowledge of the system should be limited by implementing controls over access to system documentation and manuals.

• Controls should exist for data transmitted from remote locations, such as sales in one location that update accounts receivable files at another location. The sending location should transmit control information, such as transaction control totals, to enable the receiving location to verify the update of its files. When

practical, central monitoring should ensure that all remotely processed data have been received completely and updated accurately.

• When replicated files exist at multiple locations, controls should ensure that all files used are correct and current and, when data are used to produce financial information, that no duplication arises.

Remote Access Security

Remote access connectivity to their information resources is required for many organizations for different types of users, such as employees, vendors, consultants, business partners and customer representatives. In providing this capability, a variety of methods and procedures are available to satisfy an organization's business need for this level of access.

Remote access users can connect to their organization's networks with the same level of functionality that exists within their office. In doing so, the remote access design uses the same network standards and protocols applicable to the systems that they are accessing, Transmission Control Protocol/Internet Protocol (TCP/IP)-based systems and systems network architecture (SNA) systems, for the mainframe where the user uses terminal emulation software to connect to a mainframe-based legacy application.

Support for these connections includes asynchronous point-to-point modem connectivity, integrated services digital network (ISDN) dial-on-demand connectivity, and dedicated lines (e.g., frame relay and digital subscriber lines

[DSL]).

Common Connectivity Methods for Remote Access

TCP/IP Internet-based remote access is a cost-effective approach that enables organizations to take advantage of the public network infrastructures and

connectivity options available, under which Internet service providers (ISPs) manage modems and dial-in servers, and DSL and cable modems reduce costs further to an organization. To effectively use this option, organizations establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Available VPN technologies apply the Internet Engineering Task Force (IETF) IPSec standard.

Advantages are their ubiquity, ease of use, inexpensive connectivity, and read, inquiry or copy only access. Disadvantages include that they are significantly less reliable than dedicated circuits, lack a central authority, and can be difficult to troubleshoot.

Organizations should be aware that using VPNs to allow remote access to their systems can create holes in their security infrastructure. The encrypted traffic can hide unauthorized actions or malicious software that can be transmitted through such channels. Intrusion detection systems (IDSs) and virus scanners able to decrypt the traffic for analysis and then encrypt and forward it to the VPN endpoint should be considered as preventive controls.

A good practice is to terminate all VPNs to the same endpoint in a VPN

concentrator and not accept VPNs directed at other parts of the network.

A less common method is to use dial-up lines (modem asynchronous point-to-point or ISDN) in accessing an organization's network access server (NAS) that works in concert with an organization's network firewall and router configuration. The NAS handles user authentication, access control and accounting, while maintaining connectivity. The most common protocol for doing this is the Remote Access Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS). In a typical NAS implementation, calls into the network are received, and as a good security practice, the call is terminated after recording the calling number and performing preliminary authentication procedures. The standard security practice has been for the NAS to initiate a call back to a predetermined number of the user. This control can be circumvented through effective implementation of call-forwarding mechanisms.

Dial-up connectivity, not based on centralized control and least preferred from a security and control standpoint, is an organization's server whose OS

is set up to accept remote access, which is referred to as a remote access server (RAS). The latter approach is not recommended, as it is extremely difficult to control remote access from many servers using its own RAS

capability.

Advantages of dial-up connectivity are its low end-user costs (local phone calls)

and that it is intuitive and easy to use (familiarity). Disadvantages are related to performance; for example, reliability in establishing connections with the NAS (phone networks' electrical interference) and time-sensitive media-rich applications or a service's failure when data-rate throughput is low.

Another common connectivity method often used for remote access is dedicated network connections. Using private, often proprietary, network circuits is the approach generally considered the safest because the only network traffic carried belongs to the same organization. It is commonly used by branch/regional offices or with business partners. Advantages of dedicated network connections include greater performance gains in data throughput and reliability, and data on a dedicated link belonging to the subscribing organization, where an intruder would have to compromise the

telecommunications provider itself to access the data link. A disadvantage is that cost is typically two- to five-times higher than connections to the Internet.

Remote access risk includes the following:

• Denial of service (DoS)—remote users may not be able to gain access to data or applications that are vital for them to carry out their day-to-day business

• Malicious third parties—these may gain access to critical applications or sensitive data by exploiting weaknesses in communications software and network protocols

• Misconfigured communications software—may result in unauthorized access or modification of an organization's information resources

• Misconfigured devices on the corporate computing infrastructure

• Host systems that are not secured appropriately—can be exploited by an intruder gaining access remotely

• Physical security issues over remote users' computers Remote access controls include the following:

• Policy and standards

• Proper authorizations

• Identification and authentication mechanisms

• Encryption tools and techniques such as use of a VPN

• System and network management

5.4.11 AUDIT LOGGING IN MONITORING SYSTEM

ACCESS

Most access control software has security features that enable a security administrator to automatically log and report all levels of access attempts—

successes and failures. For example, access control software can log computer activity initiated through a logon ID or computer terminal. This information provides management an audit trail to monitor activities of a suspicious nature, such as a hacker attempting brute force attacks on a privileged logon ID. Also, keystroke logging can be turned on for users who have sensitive access privileges. What is logged is determined by the action of the organization. Issues include what is logged, who/what has access to the logs and how long logs are retained (record-retention item).

Access Rights to System Logs

Access rights to system logs for security administrators to perform the previous activities should be strictly controlled.

Computer security managers and system administrators/managers should have access for review purposes; however, security and/or administration personnel who maintain logical access functions may not need to access audit logs.

It is particularly important to ensure the integrity of audit trail data against modification. This can be done using digital signatures, write-once devices or a SIEM system. The audit trail files need to be protected because intruders may try to cover their tracks by modifying audit trail records. Audit trail records should be protected by strong access controls to help prevent

unauthorized access. The integrity of audit trail information may be particularly important when legal issues arise, such as the use of audit trails as legal evidence. (This may, for example, require daily printing and signing of the logs.)

Questions regarding such legal issues should be directed to the appropriate legal counsel.

The confidentiality of audit trail information may also be protected if the audit trail is recording information about users that may be disclosure-sensitive, such as transaction data containing personal information (e.g., before and after records of modification to income tax data). Strong access controls and encryption can be particularly effective in preserving confidentiality.

Media logging is used to support accountability. Logs can include control numbers (or other tracking data), such as the times and dates of transfers, names and signatures of individuals involved, and other relevant information.

Periodic spot checks or audits may be conducted to determine that no controlled items have been lost and that all are in the custody of individuals named in control logs. Automated media tracking systems may be helpful for maintaining inventories of tape and disk libraries.

A periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours. Certain reports are generated for security recorded in activity logs.

Tools for Audit Trail (Logs) Analysis

Many types of tools have been developed to help reduce the amount of information contained in audit records and to delineate useful information from the raw data.

On most systems, audit trail software can create large files, which can be extremely difficult to analyze manually. The use of automated tools is likely to be the difference between unused audit trail data and an effective review.

Some of the types of tools include:

• **Audit reduction tools**—They are preprocessors designed to reduce the

volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. (This alone may cut in half the number of records in the audit trail.)

These tools generally remove records generated by specified classes of events—for example, records generated by nightly backups might be removed.

• **Trend/variance-detection tools**—They look for anomalies in user or system behavior. It is possible to construct more sophisticated processors that monitor usage trends and detect major variations. For example, if a user typically logs in at 09:00 but appears at 04:30 one morning, this may indicate a security problem that may need to be investigated.

• **Attack-signature-detection tools**—They look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt. A simple example would be repeated failed logon attempts.

• **SIEM systems**—These tools capture audit trails or logs and perform real-time analysis on them. They can aggregate audit trails and logs from many different sources. These data can then be correlated, and alerts provided if required. Some SIEM systems can also be configured to perform

automated tasks based upon the alerts (e.g., launching a vulnerability scan or commanding the firewall to close a certain port).

Cost Considerations

Audit trails involve many costs that factor into IT's determination as to how much logging is enough. First, some system overhead is incurred while recording the audit trail. Additional system overhead will be incurred to store and process the records. The more detailed the records, the more overhead is required. In some systems, logging every event could cause the system to lock up or slow to the point at which response time would be measured in minutes. Obviously, this is not acceptable if IT is properly aligned with the needs of the business. Another cost involves human and machine time required when performing the analysis. This can be minimized by using tools to perform most of the analysis. Many simple analyzers can be constructed quickly and inexpensively from system utilities, but they are limited to audit reduction and the identification of particularly sensitive events. More complex tools, such as SIEM systems, will be more expensive both to purchase and to implement.

The final cost of audit trails is the cost of investigating unexpected and anomalous events. If the system is identifying too many events as suspicious, administrators may spend undue time reconstructing events and questioning

personnel.

The frequency of the security administrator's review of computer access reports should be commensurate with the sensitivity of the computerized information being protected. The IS auditor should ensure that the logs cannot be tampered with, or altered, without leaving an audit trail.

When reviewing or performing security access follow-up, the IS auditor should look for:

• Patterns or trends that indicate abuse of access privileges, such as concentration on a sensitive application

• Violations (such as attempting computer file access that is not authorized) and/or use of incorrect passwords

When a violation is identified:

• The person who identified the violator should refer the problem to the security administrator for investigation.

• The security administrator and responsible management should work together to investigate and determine the severity of the violation.

Generally, most violations are accidental.

• If a violation attempt is serious, executive management should be notified, not law enforcement officials. Executive management normally is

responsible for notifying law enforcement officials. Involvement of external agencies may result in adverse publicity that is ultimately more damaging than the original violation; therefore, the decision to involve external agencies should be left to executive management.

• Procedures should be in place to manage public relations and the press.

• To facilitate proper handling of access violations, written guidelines should exist that identify various types and levels of violations and how they will be addressed. This effectively provides direction for judging the seriousness of a violation.

• Disciplinary action should be a formal process that is applied consistently.

This may involve a reprimand, probation or immediate termination. The

procedures should be legally and ethically sound to reduce the risk of legal action against the company.

• Corrective measures should include a review of the computer access rules, not only for the perpetrator but for interested parties. Excessive or inappropriate access rules should be eliminated.

5.4.12 NAMING CONVENTIONS FOR LOGICAL ACCESS CONTROLS

Access capabilities are implemented by security administration in a set of access rules that stipulates which users (or groups of users) are authorized to access a resource (such as a dataset or file) and at what level (such as read or update). The access control mechanism applies these rules whenever a user attempts to access or use a protected resource.

Access control naming conventions are structures used to govern user access to the system and user authority to access/use computer resources, such as files, programs and terminals. These general naming conventions and associated files are required in a computer environment to establish and maintain personal accountability and SoD in the access of data. The owners of the data or application, with the help of the security officer, usually set up naming conventions. The need for sophisticated naming conventions over access controls depends on the importance and level of security that is needed to ensure that unauthorized access has not been granted. It is important to establish naming conventions that both promote the implementation of efficient access rules and simplify security administration.

Naming conventions for system resources (e.g., as datasets, volumes, programs and employees' workstations) are an important prerequisite for efficient administration of security controls. Naming conventions can be structured so that resources beginning with the same high-level qualifier can be governed by one or more generic rule(s). This reduces the number of rules required to adequately protect resources which, in turn, facilitates security administration and maintenance efforts.

5.4.13 FEDERATED IDENTITY MANAGEMENT

Federated identity management (FIM)—also known as identity federation—

is an arrangement between multiple enterprises to use common identification data of users within a group to provide access to organization systems. A corporate entity may initiate such federation for all group enterprises within corporate control. The main objective of implementing FIM is to make access easier for users.

Identity federation links a user's identity across multiple security domains, each supporting its own identity management system. When two domains are federated, the user can authenticate to the home domain and then access resources in the other domain without having to perform a separate login process. Identity federation offers economic advantages and convenience to enterprises and their network subscribers. For example, multiple corporations can share a single application, resulting in cost-savings and consolidation of resources.

For FIM to be effective, the partners must have a sense of mutual trust, generally established through contracts. Identity authorization message transmission between partners in an FIM system must be through a secure channel.

To implement effective FIM, partnering organizations must have policies that adhere to the security requirements of all members, which can be sometimes be complicated due to different security requirements and rules set by each enterprise. Also, when an organization is a member of multiple federations, ensuring polices accurately reflect the rules of each member can be time consuming, costly and complex.

An IS auditor should review the business case that establishes need for identity federation. Next is review of policies and monitoring mechanism to ensure unauthorized access are prevented or detected and corrected.

5.4.14 AUDITING LOGICAL ACCESS

When evaluating logical access controls, the IS auditor should:

• Obtain a general understanding of the security risk facing information processing, through a review of relevant documentation, inquiry,

observation, risk assessment and evaluation techniques.

• Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness by reviewing appropriate hardware and software security features and identifying any deficiencies or redundancies.

• Test controls over access paths to determine whether they are functioning and effective by applying appropriate audit techniques.

• Evaluate the access control environment to determine if the control objectives are achieved by analyzing test results and other audit evidence.

• Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standards or practices and procedures used by other organizations.

Familiarization With the IT Environment

This is the first step of the audit and involves obtaining a clear understanding of the technical, managerial and security environment of the IS processing facility. This typically includes interviews, physical walk-throughs, review of documents and risk assessments.

Assessing and Documenting the Access Paths

The access path is the logical route an end user takes to access computerized information. This starts with a terminal/workstation and typically ends with the data being accessed. Along the way, numerous hardware and software components are encountered. The IS auditor should evaluate each component for proper implementation and physical and logical access security.

Special consideration should be given to the:

• Origination and authorization of the data

• Validity and correctness of the input data

• Maintenance of the affected OSs (patching, hardening and closing the

unnecessarily open ports)

The typical sequence of the components follows:

1. An end user signs on to a PC, which is part of the LAN. The PC should be physically secure, and the logon ID/password that is used for sign-on

should be subject to the restrictions identified previously.

• The OS running on the PC should be patched according to the

suggestions of the supplier of the OS and the malware defense must also be updated. Out-of-date OS versions and out-of-date virus defenses can be exploited by attackers. The PC OS must be hardened—deleting the unnecessary services (e.g., those connected with remote procedure calls, sending mail, or network management) and library routines. The parameter settings and configuration of the OS must also be

investigated. The ports that are not used should be closed.

2. One or more servers on which the applications are to be used are invoked.

The OS running on the servers should be patched according to the recommendations of the supplier of the OS and the virus defense must also be updated. Out-of-date OS versions and out-of-date virus defenses can be exploited by attackers. The server OS must be hardened—deleting unnecessary services (e.g., those connected with remote procedure calls, sending mail, or network management) and library routines. The

parameter settings and configuration of the OS must also be investigated.

The ports that are not used should be closed.

3. The telecommunications software (LAN server or terminal emulator if connecting to a mainframe) intercepts the logon to direct it to the appropriate telecommunication link. The telecommunication software can restrict PCs to specific data or application software. A key audit issue with telecommunication software is to ensure that all applications have been defined within the software and that the various optional

telecommunication control and processing features used are appropriate and approved by management. This analysis typically requires the assistance of a system software analyst.

4. The transaction processing software may be the next component in the access path. This software routes transactions to the appropriate application software. Key audit issues include ensuring proper

identification/authentication of the user (logon ID and password) and authorization of the user to gain access to the application. This analysis is performed by reviewing internal tables that reside in the transaction processing software or in separate security software. Access to these should be restricted to the security administrator.

5. The application software is encountered and should process transactions in

accordance with program logic. Audit issues include restricting access to the production software library to only the implementation coordinator.

6. The database management system (DBMS) directs access to the

computerized information. Audit issues include ensuring that all data elements are identified in the data dictionary, that access to the data dictionary is restricted to the database administrator (DBA) and that all data elements are subject to logical access control. The application data now can be accessed.

7. The access control software can wrap logical access security around all of the above components. This is done via internal security tables. Audit issues include ensuring all of the above components are defined to the access control software, providing access rules that define who can access what on a need-to-know basis and restricting security table access to the security administrator.

Note: The development of the application systems must be disciplined.

The IS auditor should evaluate the control objectives, referring to the origination and authorization of the applications data, and should evaluate the control measures used in data input and processing. Omitting these control objectives and measures makes the applications vulnerable to attacks either from within or from the outside, especially from the Internet.

Firewalls do not protect applications against the types of attacks that come with the HTTP communication that is usually permitted on the

applications.

Interviewing Systems Personnel

Technical experts are often required to control and maintain the various components of the access path, as well as the OS and computer mainframe.

These people can be a valuable source of information to the IS auditor when gaining an understanding of security. To determine who these people are, the IS auditor should meet with the IS manager and review organizational charts and job descriptions. Key people include the security administrator, network control manager and systems software manager.

The security administrator should be asked to identify the responsibilities and

functions of the position. If the answers provided to this question do not support sound control practices or do not adhere to the written job description, the IS auditor should compensate by expanding the scope of the testing of access controls. Also, the IS auditor should determine whether the security administrator is aware of the logical accesses that must be protected, has the motivation and means to actively monitor logons to account for employee changes, and is knowledgeable in how to maintain and monitor access.

A sample of end users should be interviewed to assess their awareness of management policies regarding logical security and confidentiality.

Reviewing Reports From Access Control Software

The reporting features of access control software provide the security administrator with the opportunity to monitor adherence to security policies.

By reviewing a sample of security reports, the IS auditor can determine whether enough information is provided to support an investigation and if the security administrator is performing an effective review of the report.

Unsuccessful access attempts should be reported and should identify the time, terminal, logon and file or data element for which access was attempted.

Reviewing Application Systems Operations Manual

An application systems manual should contain documentation on the programs that generally are used throughout a data processing installation to support the development, implementation, operations and use of application systems. This manual should include information about the platform the application can run on, DBMSs, compilers, interpreters, telecommunication monitors and other applications that can run with the application.

5.4.15 DATA LEAKAGE

Data leakage involves siphoning or leaking information out of the computer.

This includes dumping files to paper or stealing computer reports and tapes.

Unlike product leakage, data leakage leaves the original copy, so it may go undetected.

Fundamentally, data leakage involves the unauthorized transfer of sensitive or proprietary information from an internal network to the outside world.

Ways that this information can leave the enterprise include peer-to-peer (P2P) networks, instant message (IM), social media, email, cloud storage and file sharing solutions.

Common controls to prevent data leakage have also been covered including identifying assets, classifying them and an information security management system, including policies and procedures.

Despite these controls, many enterprises still leak sensitive information.

These leaks create risk to enterprises, their customers and business partners, and can negatively impact an enterprise’s reputation, compliance, competitive advantage and finances.

Concerns over the need to better control and protect sensitive information have given rise to a new set of solutions. These solutions vary in their capabilities and methodologies, but collectively they have been placed in a category known as data leak prevention (or protection).

Data Leak Prevention

Data leak prevention (DLP) is suite of technologies and associated processes that locate, monitor and protect sensitive information from unauthorized disclosure. Most DLP solutions include a suite of technologies that facilitates the following three key objectives:

• Locate and catalog sensitive information stored throughout the enterprise.

• Monitor and control the movement of sensitive information across enterprise networks.

• Monitor and control the movement of sensitive information on end-user systems.

These objectives are associated with the following three primary states of information:

• Data at rest

• Data in motion

• Data in use

Each of these three states of data is addressed by a specific set of technologies provided by DLP solutions.

Data at Rest

A basic function of DLP solutions is the ability to identify and log where specific types of information (e.g., credit card or social security numbers) are stored throughout the enterprise. To accomplish this, most DLP systems use crawlers, which are applications that are deployed remotely to log onto each end system and “crawl” through data stores, searching for and logging the location of specific information sets based on a set of rules that have been entered into the DLP management console.

Data in Motion (Network)

To monitor data movement on enterprise networks, DLP solutions use specific

network appliances or embedded technology to selectively capture and analyze network traffic. When files are sent across a network they are typically broken into packets. To inspect the information being sent across the network the DLP solution must be able to passively monitor the network traffic, recognize the correct data streams to capture, assemble the collected packets, reconstruct the files carried in the data stream, and perform the same analysis that is done on the data at rest to determine whether any portion of the file contents is restricted by its rule set. At the core of this ability is a process known as deep packet inspection (DPI). DPI goes beyond the basic header information of a packet to read the contents within the packet's payload (akin to a letter within a postal envelope). If sensitive data are detected flowing to an unauthorized destination, the DLP solution has the capability to alert and optionally block the data flows in real or near real time, again based on the rule set defined within its central management component.

Based on the rule set, the solution may also quarantine or encrypt the data in question.

Data in Use (Endpoint)

Data in use primarily refers to monitoring data movement stemming from actions taken by end users on their workstations, whether that would entail

copying data to a flash drive, sending information to a printer or even cutting and pasting between applications. DLP solutions typically accomplish this through the use of a software program known as an agent, which is ideally controlled by the same central management capabilities of the overall DLP

solution.

To be considered a full DLP solution, the capability to address the three states of information must exist and be integrated by a centralized management function. The range of services available in the management console varies between products but many have functions in common, such as those outlined in the following sections.

Policy Creation and Management

Policies (rule sets) dictate the actions taken by the various DLP components.

Most DLP solutions come with preconfigured policies (rules) that map to common regulations. It is just as important to be able to customize these policies or build completely custom policies. These should be built upon the asset management and data classifications exercises performed by the enterprise.

Directory Services Integration

Integration with directory services allows the DLP console to map a network address to a named end user.

Workflow Management

Most full DLP solutions provide the capacity to configure incident handling, allowing the central management system to route specific incidents to the appropriate parties based on violation type, severity, user and other such criteria.

Backup and Restore

Backup and restore features allow for preservation of policies and other configuration settings.

Reporting

A reporting function may be internal or may leverage external reporting tools.

DLP Risk, Limitations and Considerations

• **Improperly tuned network DLP modules**—Proper tuning and testing of the DLP system should occur before enabling actual blocking of content.

Enabling the system in monitor-only mode allows for tuning and provides the opportunity to alert users to out-of-compliance processes and activities, so they may adjust accordingly. Involving the appropriate business and IT

stakeholders in the planning and monitoring stages helps to ensure that disruptions to processes will be anticipated and mitigated. Finally, establish some means of accessibility in the event there is critical content being blocked during off-hours when the team managing the DLP solution is not available.

• **Excessive reporting and false positives**—Similar to an improperly configured

IDS, DLP solutions may register significant amounts of false positives, which overwhelm staff and can obscure valid hits. Avoid excessive use of template patterns or black box solutions that allow for little customization. The greatest feature of a DLP solution is the ability to customize rules or templates to specific organizational data patterns. It is also important that the system be rolled out in phases, focusing on the highest risk areas first. Trying to monitor too many data patterns or enabling too many detection points early on can quickly overwhelm resources.

• **Encryption**—DLP solutions can only inspect encrypted information that they can first decrypt. To do this, DLP agents, network appliances and crawlers must have access to, and be able to use, the appropriate decryption keys. If users have the ability to use personal encryption packages where keys are not managed by the enterprise and provided to the DLP solution, the files cannot be analyzed. To mitigate this risk, policies should forbid the installation and use of encryption solutions that are not centrally managed, and users should be educated that anything that cannot be decrypted for inspection (meaning that the DLP solution has the encryption key) will ultimately be blocked.

• **Graphics**—DLP solutions cannot intelligently interpret graphics files.

Short of blocking or manually inspecting all such information, a significant gap will exist in an enterprise's control of its information. Sensitive information scanned into a graphics file or intellectual property that exists

in a graphics format, such as design documents, would fall into this category. Enterprises that have significant intellectual property in a graphics format should develop strong policies that govern the use and dissemination of this information. Although DLP solutions cannot intelligently read the contents of a graphics file, they can identify specific file types, their source and destination. This capability, combined with well-defined traffic analysis, can flag uncharacteristic movement of this type of information and provide some level of control.

5.5 NETWORK AND END-POINT SECURITY

Enterprises can effectively prevent and detect most attacks on their networks by employing perimeter security controls. Firewalls and IDSs provide protection and critical alert information at borders between trusted and untrusted networks.

The proper implementation and maintenance of firewalls and IDSs is critical to a successful, in-depth security program. The security landscape is filled with technologies and solutions to address a myriad of needs. Understanding the solution's function and its application to the underlying infrastructure requires knowledge of the infrastructure itself and the protocols in use.

5.5.1 IS NETWORK INFRASTRUCTURE

IS networks were developed from the need to share information resources residing on different computer devices, which enabled organizations to improve business processes and realize substantial productivity gains.

Generally, the telecommunication links or lines for networks are digital, although analog may still be used. They are classified according to the type of provider or the type of technology. Typically, they can be divided into dedicated circuit (also known as leased lines) and switched circuit.

A **dedicated circuit** is a symmetric telecommunications line connecting two locations. Each side of the line is permanently connected to the other.

Dedicated circuits can be used for telephone, data or Internet services.

A **switched circuit** does not permanently connect two locations and can be

set up on demand, based on the addressing method. There are two main types of switching mechanisms: circuit switching and packet switching.

The **circuit switching** mechanism is typically used over the telephone network (plain old telephone service [POTS], integrated services digital network [ISDN]). Switched circuits allow data connections that can be initiated when needed and terminated when communication is complete. This works much like a normal telephone line works for voice communication.

ISDN is a good example of circuit switching. When a router has data for a remote site, the switched circuit is initiated with the circuit number of the remote network. In the case of ISDN circuits, the device places a call to the telephone number of the remote ISDN circuit. When the two networks are connected and authenticated, they can transfer data. When the data transmission is complete, the call can be terminated.

Packet switching is a technology in which users share common carrier resources. Because this allows the carrier to make more efficient use of its infrastructure, the cost to the customer is generally much lower than with leased lines. In a packet switching setup, networks have connections into the carrier's network, and many customers share the carrier's network. The carrier can then create virtual circuits between customers' sites by which packets of data are delivered from one to the other through the network. The section of the carrier's network that is shared is often referred to as a cloud.

Some examples of packet-switching networks include asynchronous transfer mode (ATM), frame relay, Switched Multimegabit Data Services (SMDS) and X.25.

Methods for transmitting signals over analog telecommunication links or lines are either baseband or broadband, as described below:

• **Baseband**—The signals are directly injected on the communication link (no modulation or shift in the range of frequencies of the signal).

Generally, only one communication channel is available at any a time (half-duplex), although full-duplex modems are now available.

• **Broadband network**—Different carrier frequencies defined within the available band can carry analog signals, such as those generated by image processors or a data modem, as if they were placed on separate baseband

channels. Interference is avoided by separating adjacent carrier frequencies with a gap that depends on the band requirements of the carried signals.

The possibility of vectoring multiple independent channels on a single-carrier media enhances considerably the effectiveness of remote

connections. The condition when simultaneous data or control

transmission/reception takes place between two stations is called a full-duplex connection.

5.5.2 ENTERPRISE NETWORK ARCHITECTURES

Modern networks are part of a large, centrally managed, internetworked

architecture solution of high-speed local- and wide-area computer networks serving organizations' client server–based environments. Such architectures include clustering common types of IT functions in network segments, each uniquely identifiable and specialized to a task. For example, network segments or blocks may include web-based front-end application servers (public or private), application and database servers, and mainframe servers using terminal emulation software to allow end users to access these backend legacy-based systems. In turn, end users can be clustered together within their own network LANs, but with rapid access capabilities to incorporate information resources.

Some organizations implement service-oriented architectures (SOA), in which web software components, using Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML), interoperate in a loosely connected and distributed fashion across the network. Within this environment, information is highly accessible, available anytime and anywhere, and centrally managed for highly effective and efficient troubleshooting and performance management to achieve optimum use of network resources.

To understand the network architecture solutions offered from a business, performance and security design standpoint, an IS auditor must understand information technologies associated with the design and development of a telecommunications infrastructure (e.g., LAN and WAN specifications).

Telecommunications is the electronic transmission of data, sound and images between connected end systems (two or more computers acting as sender and

receiver). This process is enabled by a communications subsystem, such as a network interface card that interfaces each end user's computer to a common transmission medium, and network devices, such as bridges, switches and routers, to connect computers residing on different networks.

5.5.3 TYPES OF NETWORKS

The types of networks common to organizations include the following:

• **Personal area networks (PANs)**—Generally, a PAN is a microcomputer network used for communications among computer devices (including telephones, tablets, printers, cameras, scanners, etc.) being used by an individual person. The extent of a PAN is typically within a range of 33

feet (about 10 meters). PANs can be used for communication among the personal devices themselves or to connect to a higher-level network and the Internet. PANs may be wired with computer buses, such as USB. Wireless PANs (WPANs) can be set up using network technologies, such as infrared data association (IrDA) and Bluetooth (piconet) A piconet is composed of up to eight active devices in a master-slave relationship. A piconet typically has a range of 32.8 feet (10 meters), although ranges of up to 328

feet (100 meters) can be reached under ideal circumstances.

• **LANs**—LANs are computer networks that cover a limited area, such as a home, office or campus. Characteristics of LANs are higher data transfer rates and smaller geographic range. Ethernet and Wi-Fi (WLANs) are the two most common technologies currently used.

• **Storage area networks (SANs)**—SANs are a variation of LANs and are dedicated to connecting storage devices to servers and other computing devices. SANs centralize the process for the storage and administration of data.

• **Wide area networks (WANs)**—WANs are computer networks that cover a broad area, such as a city, region, nation or an international link. The Internet is the largest example of a WAN. WANs are used to connect LANs and other types of networks together so that users and computers in one location can communicate with users and computers in other locations.

Many WANs are built for one particular organization and are private.

Others, built by ISPs, provide connections from an organization’s LAN to the Internet. WANs may also be wireless (WWANs).

• **Metropolitan Area Networks (MANs)**—MANs are WANs that are limited to a city or region; usually, MANs are characterized by higher data transfer rates than WANs.

5.5.4 NETWORK SERVICES

Network services are functional features made possible by appropriate OS

applications. They allow orderly utilization of the resources on the network.

Instead of having a single OS that controls its own resources and shares them with the requesting programs, the network relies on standards and on a specific protocol or set of rules, enacted and operated through the basic system software of the various network devices that are capable of supporting the individual network services. Users and business applications can request network services through specific calls/interfaces. The following are common network application services:

• **Network file system**—Allows users to share files, printers and other resources in a network.

• **Email services**—Provide the ability, via a terminal or PC connected to a communication network, to send an unstructured message to another individual or group of people.

• **Print services**—Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network.

• **Remote access services**—Provide remote access capabilities where a computing device appears, as if directly attached to the remote host.

• **Directory services**—Store information about the various resources on a network and help network devices locate services, much like a

conventional telephone directory.

– Directory services also help network administrators manage user access to network resources.

• **Network management**—Provides a set of functions to control and maintain the network.

– Network management provides detailed information about the status of all components in the network, such as line status, active terminals, length of message queues, error rate on a line and traffic over a line. It enables computers to share information and resources within a network

and provides network reliability.

– It provides the operator with an early warning signal of network problems before they affect network reliability, allowing the operator to take timely preventive or remedial actions.

• **Dynamic Host Configuration Protocol (DHCP)**—Used by networked computers (clients) to obtain IP addresses and other parameters, such as the default gateway, subnet mask and IP addresses of domain name systems (DNSs) from a DHCP server.

– The DHCP server ensures that all IP addresses are unique (e.g., no IP

address is assigned to a second client while the first client's assignment is valid [its lease has not expired]). Thus, IP address pool management is performed by the server and not by a human network administrator.

• **DNS**—Translates the names of network nodes into network (IP) addresses.

5.5.5 NETWORK STANDARDS AND PROTOCOLS

Network architecture standards facilitate the process of creating an integrated environment that applications can work within by providing a reference model that organizations can use for structuring intercomputer and network communication processes.

Besides the convenience of using compatible architectures, one major advantage of network standards is that they help organizations meet the challenge of designing and implementing an integrated, efficient, reliable, scalable and secure network of LANs and WANs with external connectivity (public Internet). This is a major challenge due to the requirements of the following:

• **Interoperability**—Occurs when connecting various systems to support communication among disparate technologies where different sites may use different types of media that may operate at differing speeds

• **Availability**—Means end users have continuous, reliable and secure service (24/7 access)

• **Flexibility**—Needed for network scalability to accommodate network expansion and requirements for new applications and services

• **Maintainability**—Means an organization provides centralized support and troubleshooting over heterogeneous, but highly integrated systems

To accomplish these tasks, organizations need to have the ability to define specifications for the types of networks to be established (e.g., LANs/WANs) when creating an integrated environment that their applications can work within. Organizations must also provide centralized support and

troubleshooting over heterogeneous, but highly integrated systems.

5.5.6 OSI ARCHITECTURE

The purpose of network architecture standards is to facilitate this process by providing a reference model that organizations can use for building intercomputer and network communication processes, respectively.

The benchmark standard for this process, the Open Systems Interconnection (OSI) reference model, was developed by the International Organization for Standardization (ISO) in 1984. OSI is a proof-of-concept model composed of seven layers, each specifying particular specialized tasks or functions. Each layer is self-contained and relatively independent of the other layers in terms of its particular function. This enables solutions offered by one layer to be updated without adversely affecting the other layers.

The objective of the OSI reference model is to provide a protocol suite used to develop data-networking protocols and other standards to facilitate multivendor equipment interoperability. The OSI program was derived from a need for international networking standards and was designed to facilitate communication between hardware and software systems despite differences in underlying architectures.

It is important to note that in the OSI model each layer communicates not only with the layers above and below it in the local stack, but also with the same layer on the remote system. For example, the application layer on the local system appears to be communicating with the application layer on the remote system. All of the details of how the data are processed further down the stack are hidden from the application layer. This is true at every level of the model. Each layer appears to have a direct (virtual) connection to the same layer on the remote system.

The **application layer** provides a standard interface for applications that must

communicate with devices on the network (e.g., print files on a network-connected printer, send an email or store data on a file server). Thus, the application layer provides an interface to the network. In addition, the application layer may communicate the computer's available resources to the rest of the network. The application layer should not be confused with application software. Application software uses the application layer interface to access network-connected resources.

The **presentation layer** transforms data to provide a standard interface for the application layer and provides common communication services, such as encryption, text compression and reformatting (e.g., conversion of Extended Binary-coded for Decimal Interchange Code [EBCDIC] to ASCII code). The presentation layer converts the outgoing data into a format acceptable by the network standard and then passes the data to the session layer. Similarly, the presentation layer converts data received from the session layer into a format acceptable to the application layer.

The **session layer** controls the dialogs (sessions) between computers. It establishes, manages and terminates the connections between the local and remote application layers. All conversations, data exchanges and dialogs between the application layers are managed by the session layer.

The **transport layer** provides reliable and transparent transfer of data between end points, end-to-end error recovery and flow control. The transport layer ensures that all of the data sent to it by the session layer are successfully received by the remote system's transport layer. The transport layer is responsible for acknowledging every data packet received from the remote transport layer, ensuring that an acknowledgement is received from the remote transport layer for every packet sent. If an acknowledgement is not received for a packet, then that packet will be resent.

The **network layer** creates a virtual circuit between the transport layer on the local device and the transport layer on the remote device. This is the layer of the stack that understands IP addresses and is responsible for routing and forwarding. This layer prepares the packets for the data link layer.

The **data link layer** provides for the reliable transfer of data across a physical

link. It receives packets of data from the network layer, encapsulates them into frames and sends them as a bit stream to the physical layer. These frames consist of the original data and control fields necessary to provide for synchronization, error detection and flow control. Error detection is accomplished through the use of a cyclic redundancy check (CRC) that is calculated for and then added to each frame of data. The receiving data link layer calculates the CRC value for the data portion of the received frame and discards the frame if the calculated and received values do not match. A CRC

calculation will detect all single-bit and most multiple-bit errors.

A bit stream received from the physical layer is similarly converted to data packets and sent to the network layer. The data link layer logically connects to another device on the same network segment using a MAC address. Each device on the network has a unique MAC hardware address that is assigned to it at the time of manufacture. The MAC address can be overridden, but this practice is not recommended. The data link layer normally only listens to data intended for its MAC address. An important exception to this rule is that a network interface may be configured as a promiscuous interface, which will listen to all data that the physical layer sends it.

The **physical layer** provides the hardware that transmits and receives the bit stream as electrical, optical or radio signals over an appropriate medium or carrier. This layer defines the cables, connectors, cards and physical aspects of the hardware required to physically connect a device to the network. Error correction and detection is not usually implemented in the physical layer, with a few notable exceptions. Cell phones and digital microwave systems will typically implement some form of error correction code, not only detecting but actually correcting errors. The most sophisticated forms of these are used by the US National Aeronautics and Space Administration (NASA) program for communicating with its deep space probes.

ISO formulated the OSI model to establish standards for vendors developing protocols supporting open system architecture. The intent is to make different proprietary systems work seamlessly within the same network. The actual implementation of the functions defined in each layer is based on protocols

developed for each layer. A protocol is an agreed-upon set of rules and procedures to follow when implementing the tasks associated with a given layer

of the OSI model.

The intent of the OSI model is to provide a standard interface at each layer and to ensure that each layer does not have to be concerned with the details of how the other layers are implemented.

This approach supports system-to-system communication (peer-to-peer relationship) where each layer on the sender side provides information to its peer layer on the receiving side. The process also is characterized as a data traversal process with the following actions occurring:

• Data travels down through layers at the local end.

• Protocol-control information (headers/trailers) is used as an envelope at each layer to pick up control information.

• Data travels up through the layers at the receiving/destination end.

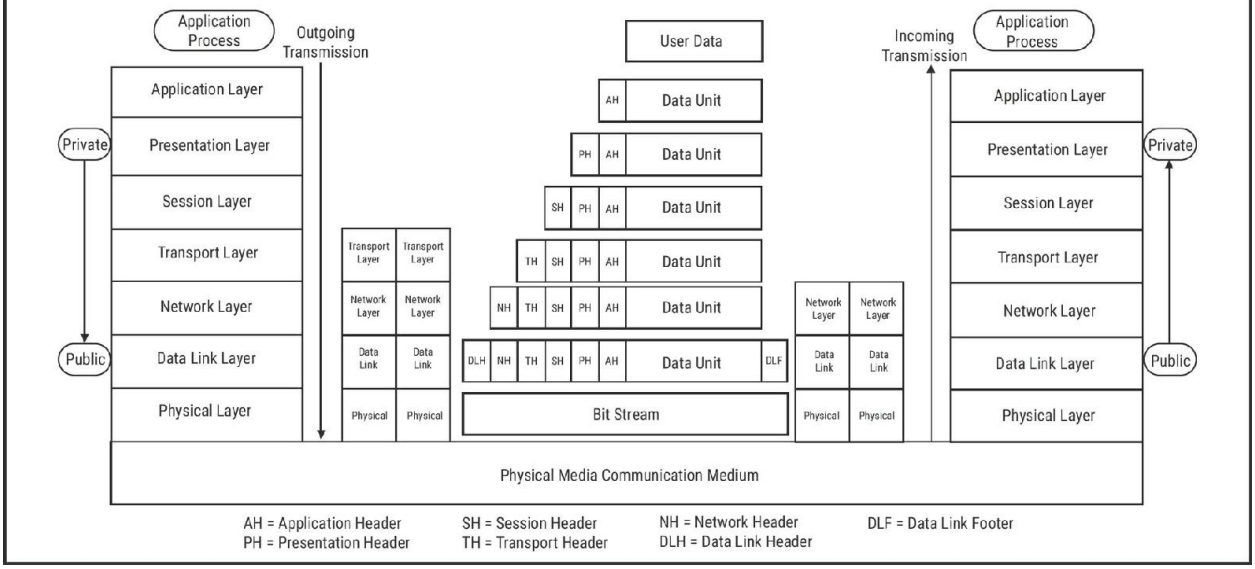
• Protocol-control information (headers/trailers) is removed as the information is passed up.

A traditional OSI model showing this process is depicted in **figure 5.10.**

5.5.7 APPLICATION OF THE OSI MODEL IN NETWORK ARCHITECTURES

The concepts of the OSI model are used in the design and development of organizations' network architectures. This includes LANs, WANs, MANs and use of the public TCP/IP-based global Internet. The following sections will provide a detailed technical discussion of each and will show how the OSI reference model applies to the various architectures. The discussion will focus on:

Figure 5.10—Traditional OSI Model



• LAN

• WAN

• Wireless networks

• Public global Internet infrastructure

• Network administration and control

• Applications in a networked environment

• On-demand computing

Local Area Network

A LAN covers a small, local area—from a few devices in a single room to a network across a few buildings. The increase in reasonably priced bandwidth has reduced the design effort required to provide cost-effective LAN

solutions for organizations of any size.

New LANs are almost always implemented using switched Ethernet (802.3).

Twisted-pair cabling (100-Base-T or better and wireless LANs [WLANs])

connects floor switches to the workstations and printers in the immediate area. Floor switches can be connected to each other with 1000-Base-T or fiber-optic cabling. In larger organizations, the floor switches may be connected to larger, faster switches whose purpose is to properly route the switch-to-switch data.

As LANs get larger and traffic increases, the requirement to carefully plan the logical configuration of the network becomes more and more important.

Network planners need to be highly skilled and very knowledgeable. Their tools include traffic monitors that allow them to monitor traffic volumes on critical links. Tracking traffic volumes, error rates and response times is every bit as important on larger LANs as it is on distributed servers and mainframes.

LAN Design Fundamentals and Specifications

To set up a LAN, an organization must assess cost, speed, flexibility and reliability. The issues include:

• Assessing media for physically transmitting data

• Assessing methods for the physical network medium

• Understanding from a performance and security standpoint how data will be transmitted across the network and how the actual LAN network is organized and structured in terms of optimizing the performance of the devices connected to it

Network Physical Media Specifications

Physical media used to connect various types of computing devices together in a network include:

• Twisted pairs

• Fiber optics for high-capacity and specific architectures

• Infrared and radio (wireless)

The type and characteristics of physical media (e.g., speed, sensitivity to external disturbances, signal loss and propagation, security) not only affect the cost of

implementation and support but also impact the capacity, flexibility and reliability of the network.

LANs can be implemented using various types of media, including:

• **Copper (twisted-pair) circuits**—Two insulated wires are twisted around each other, with current flowing through them in opposite directions. This reduces the opportunity for cross talk between pairs in the same bundle and allows for lower sensitivity to electromagnetic disturbances (shielded twisted-pair circuits) within each individual pair. Twisted-pair circuits can

also be used for some dedicated data networks. Today, the common standards for twisted-pair circuits are CAT5e, CAT6 and CAT7.

Organizations should buy certified cables from reputable suppliers and segment problem areas with switches. Additionally, assurance should be provided that maximum cabling lengths are not exceeded since this will produce intermittent failures. A disadvantage of unshielded twisted-pair cabling is that it is not immune to the effects of electromagnetic interference (EMI) and should be run in dedicated conduits, away from sources of potential interference, such as fluorescent lights. Parallel runs of cable over long distances should also be avoided since the signals on one cable can interfere with signals on adjacent cables—an EMI condition known as cross talk.

• **Fiber-optic systems**—Glass fibers are used to carry binary signals as flashes of light. Fiber-optic systems have a low transmission loss as compared to twisted-pair circuits. Optical fibers do not radiate energy nor conduct electricity. In addition, they are not affected by EMI and present a significantly lower risk of security problems, such as wiretaps. Optical fiber is a more fragile medium and is more attractive for applications where changes are infrequent. Optical fiber is smaller and lighter than metallic cables of the same capacity. Fiber is the preferred choice for high-volume, longer-distance runs. One example would be using fiber to connect floor switches to enterprise data switches. In addition, fiber-optic cable is often used to connect servers to SANs.

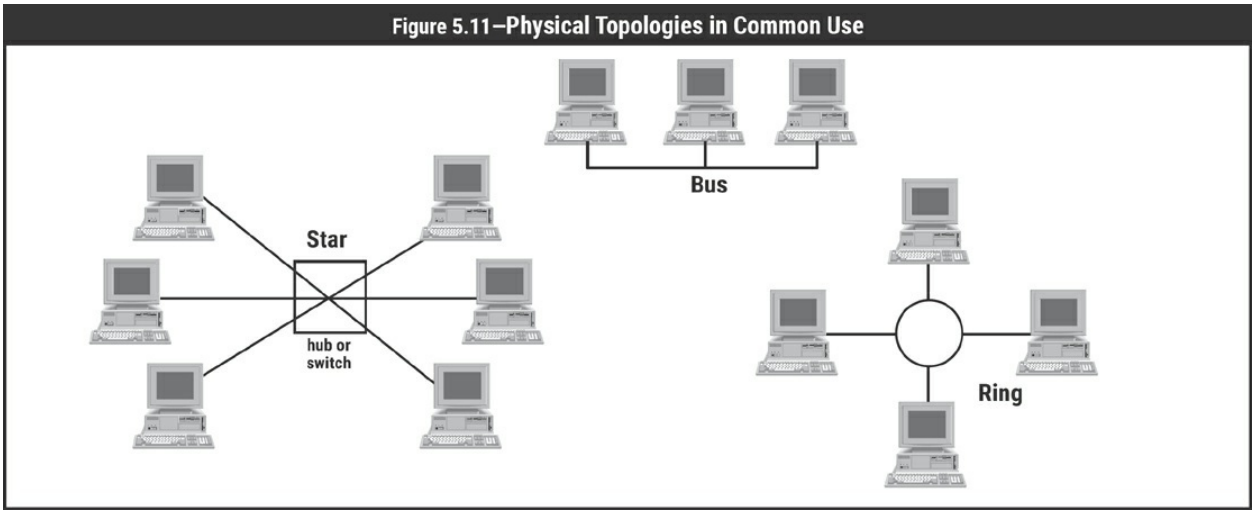
• **Radio systems (wireless)**—Data are communicated between devices using low-powered systems that broadcast (or radiate) and receive

electromagnetic signals representing data.

LAN Topologies and Protocols

LAN topologies define how networks are organized from a physical standpoint, whereas protocols define how information transmitted over the network is interpreted by systems.

LAN physical topology was previously tied fairly tightly to the protocols that were used to transfer information across the wire. This is no longer true. For current technology, the physical topology is driven by ease of construction, reliability and practicality. Of the physical topologies that have been



commonly used—bus, ring and star—only the star is used to any great extent in new construction. **Figure 5.11** illustrates commonly used physical topologies.

LAN Media Access Technologies

LAN media access technologies for accessing physical transmission media give devices shared access to the network, while also preventing a single device from monopolizing the network.

Ethernet has evolved from its original bus configuration, providing 10 Mbps speed with two coaxial cable versions (thin and thick), to star configurations initially using 10-Base-T (Ethernet using twisted-pair cabling) and now using today's more modern versions: Fast Ethernet (100 Mbps) and Gigabit Ethernet (1 Gbps).

A critical aspect of any communication is determining the recipient of a

message. At this level, considering Fast Ethernet and Gigabit Ethernet, a media access control (MAC) address is used to specify the recipient. Every network interface that is manufactured has a unique MAC address burned into the device by the manufacturer and is only used for the last hop of any communication (see TCP/IP and Its Relation to the OSI Reference Model to see how this fits in with real-world addresses, such as 192.168.4.5). Every network interface card (NIC) connected to the network listens to every conversation on the network. Normally, a NIC device driver (software) only

collects the data with its address. A NIC that has been placed in promiscuous mode will read all data passing over the network (including user IDs and passwords).

The initial bus arrangement typically provides an effective throughput of 5

Mbps among all of the systems connected to a bus segment. Bus segments could be connected together with repeaters or bridges. Repeaters regenerate signals—allowing a longer span for the network. Bridges connect multiple buses together—blocking any traffic that could not be delivered on a given segment. Bridges also serve another critical function—that of breaking the network into multiple collision domains.

Ethernet is a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) protocol. This is analogous to a car attempting to turn into a street. The driver's view is limited to only the street in front of him/her. If nothing is visible, the driver attempts to turn on to the street. If the driver collides with another vehicle, he/she backs up and tries again later. It should be apparent that if the street is very busy, a lot of collisions would occur. Similarly, if all of the traffic is coming from one particular house, then many cars can be handled in an efficient manner. If there are cars coming from a lot of different houses, then the overall traffic volume that can be handled is much lower.

This is the way in which Ethernet behaves in a bus arrangement.

The use of coaxial cable in this example is rather problematic. The cable itself is a single point of failure. Adding a new station would not solve the problem, and there exists a distinct lack of flexibility with such an implementation.

To alleviate this problem, a physical implementation using a twisted-pair telephone cable was developed. This medium is much cheaper than coaxial cable

and can be implemented using a star topology. The first implementation has all of the points of the star connected together using an unintelligent device called a hub—basically, a panel of connectors that allows all of the wires to be joined together. Circuitry within the hub electrically disconnects any branch that is not active. A problem on a single branch can still cause problems with the entire network, but the circuitry is simpler, and a

technician can easily isolate the problem at the hub. The traffic jam problem still exists, though.

Replacing hubs with switches was a significant advance in technology. A switch is an intelligent device that provides a private path for each pair of connections on the switch. If A is transferring data to B, it can do so without requiring C to transfer data to D. Further, transfers from A to D can be handled without fear of collision. This is analogous to a traffic light on a LAN. Collisions are then only an issue if more than one car is going to the same destination, and a traffic light can manage that problem.

While the traffic volume to or from any given device is still limited to the constraints set by the used technology (e.g., 10, 100, 1000 Mbps), this volume can be maintained between many pairs of devices. Additionally, the problem of collisions is eliminated; the switch ensures that they cannot happen. A packet may be delayed—while it waits for other traffic to clear the intersection—but it never encounters a delay caused by a collision or needs to be resent.

From a security perspective, switches provide another significant improvement. Each device on the network can only see traffic destined for its MAC address and cannot eavesdrop on network traffic intended for other destinations.

Today, switches are so inexpensive that there is little justification for continuing to use hubs. Switches that provide individual devices with 100

Mbps service and provide 1 Gbps connection to higher-level switches are in common use. Switches are increasingly providing additional functionality that can be used to implement corporate security policy.

Another media access technology that was commonly used in LANs is the token ring medium access method which uses ring networks. Devices using this method gain access to the network on the basis of a unique frame, called a token, that is passed around the network. Token ring technologies have almost

disappeared in today's networks.

LAN Components

Components commonly associated with LANs are repeaters, hubs, bridges, switches and routers.

Repeaters are physical layer devices that extend the range of a network or connect two separate network segments together. Repeaters receive signals from one network segment and amplify (regenerate) the signal to compensate for signals (analog or digital) that are distorted due to a reduction of signal strength during transmission (i.e., attenuation).

Hubs are physical layer devices that serve as the center of a star-topology network or a network concentrator. Hubs can be active (if they repeat signals sent through them) or passive (if they merely split signals).

Bridges are data link layer devices that were developed to connect LANs or create two separate LAN or WAN network segments from a single segment to reduce collision domains. The two segments work as different LANs below the data link level of the OSI reference model, but from that level and above, they behave as a single logical network. Bridges act as store-and-forward devices in moving frames toward their destination. This is achieved by analyzing the MAC header of a data packet, which represents the hardware address of an NIC. Bridges can also filter frames based on Layer 2

information. For example, they can prevent frames sent from predefined MAC addresses from entering a particular network. Bridges are software-based, and they are less efficient than other similar hardware-based devices, such as switches. Therefore, bridges are not major components in today's enterprise network designs.

Layer 2 switches are data link level devices that can divide and interconnect network segments and help to reduce collision domains in Ethernet-based networks. Furthermore, switches store and forward frames, filtering and forwarding packets among network segments, based on Layer 2 MAC source and destination addresses, as bridges and hubs do at the data link layer.

Switches, however, provide more robust functionality than bridges through use of more sophisticated data link layer protocols that are implemented via

specialized hardware called application-specific integrated circuits (ASICs).

The benefits of this technology are performance efficiencies gained through

reduced costs, low latency or idle time, and a greater number of ports on a switch with dedicated high-speed bandwidth capabilities (e.g., many ports on a switch are available with 10/100 Ethernet and/or Gigabit Ethernet speeds).

Switches are also applicable in WAN technology specifications.

Routers are similar to bridges and switches in that they link two or more physically separate network segments. The network segments linked by a router, however, remain logically separate and can function as independent networks. Routers operate at the OSI network layer by examining network addresses (i.e., routing information encoded in an IP packet). By examining the IP address, the router can make intelligent decisions to direct the packet to its destination. Routers differ from switches operating at the data link layer in that they use logically based network addresses, use different network addresses/segments off all ports, block broadcast information, block traffic to unknown addresses, and filter traffic based on network or host information.

Routers are often not as efficient as switches because they are generally software-based devices and they examine every packet coming through, which can create significant bottlenecks within a network. Therefore, careful consideration should be taken as to where routers are placed within a network. This should include leveraging switches in network design as well as applying load balancing principles with other routers for performance

“efficiency considerations.

Advances in switch technology have also provided switches with operating capabilities at Layer 3 and Layer 4 of the OSI reference model. A **Layer 3**

switch goes beyond the Layer 2–MAC addressing, acting at the network layer of the OSI model like a router. The Layer 3 switch looks at the incoming packet’s networking protocol (e.g., IP). The switch compares the destination IP address to the list of addresses in its tables, to actively calculate the best way to send a packet to its destination. This creates a virtual circuit (i.e., the switch has the ability to segment the LAN within itself and will create a pathway between the receiving and the transmitting device to send the data). It then forwards the

packet to the recipient's address. This provides the added benefit of reducing the size of network broadcast domains. A

broadcast domain is the domain segment or segments where all connected devices may be simultaneously addressed by a message using a special common network address range, referred to as a broadcast address. This is needed for specific network management functions. As the broadcast domain grows larger, this may cause performance inefficiencies and major security concerns in terms of information leakage within a network (e.g., enumerating network domains and specific computers within a domain). Broadcast domains should be limited or aligned with business functional

areas/workgroups within an organization to reduce the risk of information leakage to those without a need to know where systems can be targeted, and their vulnerabilities exploited. The major difference between a router and a Layer 3 switch is that a router performs packet switching using a microprocessor, whereas a Layer 3 switch performs the switching using application ASIC hardware.

In creating separate broadcast domains, Layer 3 switches also enable the concept of establishing a VLAN. A VLAN is a group of devices on one or more logically segmented LANs. A VLAN is set up by configuring ports on a switch, so devices attached to these ports may communicate as if they were attached to the same physical network segment, although the devices are located on different LAN segments. A VLAN is based on logical rather than physical connections and, thus, allow great flexibility. This flexibility enables administrators to restrict users' access of network resources to only those specified and segment network resources for optimal performance.

In **Layer 4 switching**, some application information is considered along with Layer 3 addresses. For IP, this information includes the port numbers from protocols, such as User Datagram Protocol (UDP) and TCP. These devices, unlike Layer 3 switches, are more resource intensive since they have to store application-based protocol information. Only address information is stored at the Layer 2 and Layer 3 levels.

A Layer 4 (transport layer) switch allows for policy-based switching. With this functionality, Layer 4 switches can off-load a server by balancing traffic across a cluster of servers, based on individual session information and status.

Layer 4 through 7 switches are also known as content-switches, content services switches, web-switches or application-switches. They are typically used for load balancing among groups of servers. Load balancing can be based on Hypertext Transfer Protocol (HTTP), Secured Hypertext Transfer Protocol (HTTPS) and/or VPN, or for any application TCP/IP traffic using a specific port. Content switches can also be used to perform standard operations, such as SSL encryption/decryption to reduce the load on the servers receiving the traffic, and to centralize the management of digital certificates.

Gateways are devices that are protocol converters. Typically, they connect and convert between LANs and the mainframe, or between LANs and the Internet, at the application layer of the OSI reference model. Depending on the type of gateway, the operation occurs at various OSI layers. The most common form of gateway is a systems network architecture (SNA) gateway, converting between a TCP/IP, NetBios or Inter-network Packet Exchange (IPX) session (terminal emulator) and the mainframe.

LAN Technology Selection Criteria

Some of the more relevant selection criteria are:

• What are the applications?

• What are the bandwidth needs?

• What is the area to be covered and what are the physical constraints?

• What is the budget?

• What are the remote management needs?

• What are the security needs?

• What network redundancy/resiliency is required?

LAN Security

LANs are computer networks that cover a limited area, such as a home, office or campus. As LANs facilitate the storage and retrieval of programs and data used by a group of people, the security of the LAN is dependent on the security of its

component parts, including the OS.

Risk associated with use of LANs includes:

• Loss of data and program integrity through unauthorized changes

• Lack of current data protection through inability to maintain version control

• Exposure to external activity through poor user verification and potential public network access from remote connections

• Virus and worm infection

• Improper disclosure of data because of general access rather than need-to-know access provisions

• Illegal access by impersonating or masquerading as a legitimate LAN user

• Internal user sniffing (obtaining seemingly unimportant information, such as network addresses, from the network that can be used to launch an attack)

• Internal user spoofing (reconfiguring a network address to pretend to be a different address)

• Lack of enabled detailed automated logs of activity (audit trails)

• Destruction of the logging and auditing data

The LAN security provisions available depend on the software product, product version and implementation. Commonly available network security administrative capabilities include:

• Declaring ownership of programs, files and storage

• Limiting access under the principle of least privilege (users can only access what they need to perform their role)

• Implementing record and file locking to prevent simultaneous update

• Enforcing user ID/password sign-on procedures, including the rules relating to password length, format and change frequency

• Using switches to implement port security policies rather than hubs or non-manageable routers. This will prevent unauthorized hosts, with unknown MAC addresses, to connect to the LAN.

• Encrypting local traffic using IPSec protocol

To gain a full understanding of the LAN, the IS auditor should identify and document the following:

• Users or groups with privileged access rights

• LAN topology and network design

• LAN administrator/LAN owner

• Functions performed by the LAN administrator/owner

• Distinct groups of LAN users

• Computer applications used on the LAN

• Procedures and standards relating to network design, support, naming conventions and data security

Wide Area Network

A WAN is a data communications network that transmits information across geographically dispersed LANs, such as among plant sites, cities and nations.

WAN characteristics include:

• They are applicable to the physical and data link layers of the OSI reference model.

• Data flow can be simplex (one-way flow), half duplex (one way at a time) or full duplex (both ways at one time without turnaround delay).

• Communication lines can be either switched or dedicated.

Implementation of WANs

Fiber-optic cables are commonly used these days for most high-capacity network connections, both between buildings and between cities. Other systems that may be used include:

• **Microwave radio systems**—Microwave radio provides line-of-sight transmission of voice and data through the air. Historically, analog microwave circuits supplied the majority of long-haul low-speed data and voice transmission. This technology was used because it provided a lower-cost alternative to the low-capacity cable carrier systems of the time. Many, if not most, heavy route microwave systems have since been replaced by fiber-optic cable systems providing greatly increased capacity and greatly improved reliability at a cost per channel mile that is a tiny fraction of the cost for microwave circuits of similar capacity. All new microwave construction uses digital signals, providing greatly increased data rates and reduced error rates when compared with analog circuitry. Microwave radio circuits are still in common use on “light routes” where the economics do not favor installation of fiber. Most electrical utility companies will use microwave systems to connect their Supervisory Control and Data

Acquisition (SCADA) systems together. Design of microwave circuits must consider the physical topology of the area and the climate.

Microwave antennae must be able to “see” each other. Climate conditions, such as rainfall, can adversely affect microwave links.

• **Satellite radio link systems**—These contain several

receiver/amplifier/transmitter sections called transponders. Each transponder has a bandwidth of 36 megahertz (MHz), operates at a slightly different frequency, has individual transmitter sites and sends narrow beams of microwave signals to the satellite. Like microwaves, satellite signals can be affected by weather. Although satellite signals can carry large amounts of information at a time, the disadvantage is a bigger delay compared to all of the previous media, due to the “jump” from the earth to the satellite and back (estimated at about 300 milliseconds). **Figure 5.12**

identifies the advantages and disadvantages of each physical layer medium available to networks. These physical specifications are applicable to WAN

technologies.

WAN Message Transmission Techniques

WAN message transmission techniques include:

• **Message switching**—Sends a complete message to the concentration point for storage and routing to the destination point as soon as a

communications path becomes available. Transmission cost is based on message length.

• **Packet switching**—A sophisticated means of maximizing transmission capacity of networks. This is accomplished by breaking a message into transmission units, called packets, and routing them individually through the network, depending on the availability of a channel for each packet.

Passwords and all types of data can be included within the packet. The transmission cost is by packet and not by message, route or distance.

Sophisticated error and flow control procedures are applied to each link by the network.

• **Circuit switching**—A physical communications channel is established between communicating equipment, through a circuit-switched network.

This network can be, for instance, point-to-point (e.g., leased line) multipoint, a public-switched telephone network (PSTN) or an ISDN. The connection, once established, is used exclusively by the two subscribers for the duration of the call. The network does not provide any error or flow control on the transmitted data, so this task must be performed by the user.

Figure 5.12—Transmission Media			
Media	**Use and Distance**	**Advantages**	**Disadvantages**
Twisted Pair	• Used for short distances (< 200 feet [60.96 meters]) • Supports voice and data	• Cheap • Simple to install • Readily available • Simple to modify	• Easy to tap • Easy to splice • Cross talk • Interference • Noise
Coaxial cable	• Supports data and video	• Ease of installation • Straightforward • Readily available	• Thick • Expensive • Does not support many LANs • Distance sensitive • Difficult to modify
Fiber optics	• Used for long distances • Supports voice, data, image and video	• High bandwidth capabilities • Secure • Difficult to tap • No cross talk • Smaller and lighter than copper	• Expensive • Hard to splice • Difficult to modify
Radio systems	• Used for short distances	• Cheap	• Easy to tap • Interference • Noise
Microwave radio systems	• Line-of-sight carrier for voice and data signals	• Cheap • Simple to install • Available	• Easy to tap • Interference • Noise
Satellite radio link systems	• Uses transponders to send information	• High bandwidth and different frequencies	• Interference • Noise • Easy to tap

• **Virtual circuits**—A logical circuit between two network devices that provides for reliable data communications. Two types are available—

switched virtual circuits (SVCs) or permanent virtual circuits (PVCs).

SVCs dynamically establish on-demand connectivity and PVCs establish an always-on connection.

• **WAN dial-up services**—Dial-up services using asynchronous and synchronous connectivity are widely available and well suited for organizations with a large number of mobile users. Their disadvantages are low bandwidth and limited performance.

WAN Devices

The following devices, typically operating at either the physical or data link layer of the OSI reference model, are specific to the WAN environment.

WAN switches are data link layer devices used for implementing various WAN technologies, such as ATM, point-to-point frame relay and ISDN.

These devices are typically associated with carrier networks providing dedicated

WAN switching and router services to organizations via T-1/E-1 or T-3/E-3 connections.

Routers are devices that operate at the network layer of the OSI reference model and provide an interface between different network segments on an internal network or connects the internal network to an external network.

Modems (modulator/demodulator) are data communications equipment (DCE) devices that make it possible to use analog lines (generally, the public telephone network) as transmission media for digital networks. Modems convert computer digital signals into analog data signals and analog data back to digital. When a link is established, modems operating at both ends of it automatically negotiate the fastest and safest standard that the line and the modems themselves can use, establishing speed, parity, cryptographic algorithm and compression.

For transmission purposes, modems disassemble bytes into a sequence of bits that are sent sequentially to the line. At the receiving end, these bits must be reassembled into bytes.

A main task of the modems at both ends is to maintain their synchronization so the receiving device knows when each byte starts and ends. Two methods can be used for this purpose:

• Synchronous transmission—Bits are transmitted without interruption at a constant speed. The sending modem uses a specific character when it starts transmitting a data block to “synchronize” the receiving device. This mode allows maximum efficiency, but only if blocks are not too short. Specific technical rules must be observed to maintain synchronization.

• Asynchronous transmission—The transmitting device marks the beginning and end of a byte by sending a “start” and a “stop” bit before and after each data byte. The efficiency of the line is lower, but the asynchronous standard is simpler and works well for character and block mode

transmissions.

Access servers provide centralized access control for managing remote access dial-up services.

Channel service unit/digital service unit (CSU/DSU) interfaces at the physical

layer of the OSI reference model, data terminal equipment (DTE) to

DCE, for switched carrier networks.

Multiplexors are physical layer devices used when a physical circuit has more bandwidth capacity than required by individual signals. The multiplexor can allocate portions of its total bandwidth and use each portion as a separate signal link. It can also link several low-speed lines to one high-speed line to enhance transmission capabilities.

Methods for multiplexing data include the following:

• **Time-division multiplexing (TDM)**—Information from each data channel is allocated bandwidth, based on preassigned time slots, regardless of whether there are data to transmit.

• **Asynchronous time division multiplexing (ATDM)**—Information from data channels is allocated bandwidth as needed via dynamically assigned time slots.

• **Frequency division multiplexing (FDM)**—Information from each data channel is allocated bandwidth, based on the signal frequency of the traffic.

• **Statistical multiplexing**—Bandwidth is allocated dynamically to any data channels that have the information to transmit.

WAN Technologies

Some common types of WAN technologies used to manage the

communication links are described in the following sections.

Point-to-point Protocol

Point-to-point protocol (PPP) works in the data link layer. PPP provides a single, preestablished WAN communication path from the customer premises to a remote network, usually reached through a carrier network, such as a telephone company. PPP is a widely available remote access solution that supports asynchronous and synchronous links and operates over a wide range of media. Because PPP is more stable than the older Serial Line Internet Protocol (SLIP), PPP is the Internet standard for transmission of IP packets over serial lines. PPP

makes use of two primary protocols for operation. The first, Link Control Protocol (LCP), is used when establishing, configuring and testing the data link connection. The second, Network Control Protocol (NCP), establishes and configures different network layer protocols (e.g.,

Internetwork packet exchange [IPX]). PPP features include address notification, authentication, support for multiple protocols and link monitoring.

X.25

As a packet-switched or virtual-circuit implementation, X.25 is a telecommunication standard (ITU-T) that defines how connections between data terminal equipment and data communications or circuit terminating equipment are maintained for remote terminal access and computer communications in public data networks (PDNs). Developed in 1976, X.25

operates at the lower three layers of the OSI reference model, but is no longer widely available today, primarily because it is resource-intensive in providing error control capabilities.

Frame Relay

As a packet-switched or virtual-circuit implementation, Frame Relay is a data link layer protocol for switch devices that uses a standard encapsulation technique to handle multiple virtual circuits between connected devices. The encapsulation method is high-level data link control (HDLC) for synchronous serial links using frame characters and checksums. Frame Relay is more efficient than X.25, the protocol for which it is generally considered a replacement. Contrary to X.25, Frame Relay relies more on upper layer protocols for significant error handling processes in data transmissions.

Frame Relay is a low-cost, widely available LAN technology used in WAN

point-to-point connections.

Integrated Services Digital Network

As a circuit-switched implementation, ISDN corresponds to integrated voice, data and video and is an architecture for worldwide telecommunications. This service integrates voice, data and video communication through digital switching

and transmission over digital public carrier lines. The ISDN

technologies now implemented are narrowband (basic-rate and primary-rate, not aggregated) ISDN; broadband ISDN has never been widely implemented.

Separate channels are used for customer information (i.e., B, bearer channels

—voice, data and video) and to send signals and control information (i.e., D, data channels). ISDN uses a packet-node layered protocol, based on the

CCITT's X.25 standard. Unlike Frame Relay, it is moderately available to all.

Asynchronous Transfer Mode

As a packet-switched implementation operating at the data link layer, ATM is based on the use of a cell (a fixed-size data block) switching and multiplexing technology standard that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic). Because ATM is asynchronous, time slots are available on demand with information identifying the source of the transmission contained in the header of each ATM cell. ATM is considered relatively expensive as a dedicated leased line option in comparison to other available WAN options.

Multiprotocol Label Switching

Multiprotocol label switching (MPLS) provides a mechanism for engineering network traffic patterns that is independent of routing tables. MPLS assigns short labels to network packets that describe how to forward them through the network. MPLS is independent of any routing protocol and can be used for unicast packets.

In traditional Level 3 forwarding, as a packet travels from one router to the next, an independent forwarding decision is made at each hop. The IP

network layer header is analyzed, and the next hop is chosen based on this analysis and on the information in the routing table. In an MPLS

environment, the analysis of the packet header is performed just once, when a packet enters the MPLS cloud. The packet is then assigned to a stream, which is

identified by a label—a short (20-bit), fixed-length value at the front of the packet. Labels are used as lookup indexes into the label forwarding table.

This table stores forwarding information for each label. Additional information, such as class-of-service (CoS) values, which can be used to prioritize packet forwarding, can be associated with a label.

Digital Subscriber Lines

DSL is a network provider service using modem technology over existing twisted-pair telephone lines to transport high-bandwidth data, such as multimedia and video.

Characteristics of DSL include:

• Dedicated, point-to-point, public network access on the local loop. Local loops are generally the final segment of the path between a network service provider's (NSP) central office and the customer site.

• Delivers high-bandwidth data rates to dispersed customers at low cost through the existing telecommunications infrastructure

• Always-on access, which eliminates call setup and makes it ideal for Internet/intranet and remote LAN access

DSL services vary in their speed and type of modulation:

• Asymmetric Digital Subscriber Line (ADSL)

• Symmetric Digital Subscriber Line (SDSL)

• High Bit-rate Digital Subscriber Line (HDSL)

• High Bit-rate Digital Subscriber Line version 2 (HDSL-2)

• Single-Pair High-speed Digital Subscriber Line (SHDSL)

• G.SHDSL (an international standard for symmetric DSL also known as G.001.2)

• Very High Speed Digital Subscriber Line (VDSL)

Virtual Private Networks

A VPN extends the corporate network securely via encrypted packets sent out via virtual connections over the public Internet to distant offices, home workers, salespeople and business partners. Rather than using expensive dedicated leased lines, VPNs take advantage of the public worldwide IP

infrastructure, thereby enabling remote users to make a local call (versus dialing-in at long distance rates) or use an Internet cable modem or DSL

connections for inexpensive public network connectivity.

VPNs are platform independent. Any computer system that is configured to run on an IP network can be connected through a VPN with no modifications, except for the installation of remote software.

There are three types of VPNs:

1. **Remote-access VPN**—Connects telecommuters and mobile users to the enterprise WAN in a secure manner; it lowers the barrier to

telecommuting by ensuring that information is reasonably protected on the

open Internet.

2. **Intranet VPN**—Connects branch offices within an enterprise WAN

3. **Extranet VPN**—Gives business partners limited access to each other's corporate network; and example is an automotive manufacturer with its suppliers

The only difference between a traditional, intracompany VPN (intranet) and an intercompany VPN (extranet) is the way the VPN is managed. With an intranet VPN, all network and VPN resources are managed by a single organization. When an organization's VPN is used for an extranet, management control becomes weak. Therefore, it is recommended that in extranet VPN, each constituent company manage its own VPN and maintain control over it.

VPNs allow:

• Network managers to cost-efficiently increase the span of the corporate

network

• Remote network users to securely and easily access their corporate enterprise

• Corporations to securely communicate with business partners

• Supply chain management to be efficient and effective

• Service providers to grow their businesses by providing substantial incremental bandwidth with value-added services

Determining which network resources should be linked via a VPN depends on the applications that are used on the various systems. Requirements often used to determine network connectivity include security policies, business models, intranet server access, application requirements, data sharing and application server access.

The process of encrypting packets, which makes VPN an effective protection scheme, uses IETF's IP Security (IPSec) standard. IPSec is implemented in two modes. The IPSec tunnel mode will encrypt the entire packet, including the header. The IPSec transport mode will encrypt only the data portion of the packet. A given VPN might use IPSec tunnel mode or might use IPSec transport mode with other encryption methods for the non-data parts of the

packet.

Independent of the type of connectivity, the primary issues are:

• Security of transmissions, including preventing "hijacking" of transmissions and preventing malware from entering the network

• Managing the technology

• Configuration management

• Ensuring information is unaltered and maintains accuracy and reliability The impact on the business transmitting data through public networks and the accompanying risk are significant. Depending on the industry, enterprises may experience outages and intrusion attempts for financial gain, to obtain intellectual property, to create business disruption, to obtain sensitive private

information, or to compromise national security. The perpetrators of an intrusion can be external or internal, private government sponsored. This activity may increase the enterprise's risk of:

• Public relations issues with the customers or the public (reputational risk)

• Inability to comply with regulatory processing requirements (regulatory and financial risk)

• Inability to perform critical business functions (operational and financial risk)

• Inability to maintain payroll and employee privacy (regulatory and reputational risk)

• Loss of physical or informational assets (reputational and financial risk)

• Inability to meet contractual service level agreements (SLAs) with third parties or customers (contractual risk)

VPN technology, if properly configured, will reduce the risk associated with privileged data traversing a public network.

TCP/IP and Its Relation to the OSI Reference Model

The protocol suite used as the *de facto* standard for the Internet is known as the TCP/IP. The TCP/IP suite includes both network-oriented protocols and application support protocols. **Figure 5.13** shows some of the standards associated with the TCP/IP suite and where these fit within the ISO model. It is interesting to note that the TCP/IP set of protocols was developed before

Figure 5.13—OSI Association With the TCP/IP Suite

	OSI Model	TCP/IP Conceptual Layers	Protocol Data Unit (PDU)	TCP/IP Protocols	Equipment	Layer Functions	Layer Functions
7	Application	Application	Data	HTTP File Transport Protocol (FTP) Simple Mail Transport Protocol (SMTP) TFTP NFS Name Server Protocol (NSP) Simple Network Management Protocol (SNMP) Remote Terminal Control Protocol (Telnet) LPD X Windows DNS DHCP/BootP	Gateway	Provides user interface	File, print, message, database, and application services
6	Presentation					Presents data Handles processing such as encryption	Data encryption, compression and translation services
5	Session					Keeps separate the data of different applications	Dialog control
4	Transport	Transport	Segment	Transmission Control Protocol (TCP) User Datagram Protocol (UDP)	Layer 4 switch	Provide reliable or unreliable delivery	End-to-end connection
3	Network	Network interface	Packet	ICMP ARP RARP Internet Protocol (IP)	Route Layer 3 switch	Provides logical addressing which routers use for path determination	Routing
2	Data link	LAN or WAN interface	Frame	Ethernet Fast Ethernet FDDI Token Ring Point-to-point Protocol (PPP)	Layer 2 switch Bridge Wireless AP NIC	Combines packets into bytes and bytes into frames Provides access to media using MAC address Performs error detection, not error correction	Framing
1	Physical		Bits		Hub Repeater NIC	Moves bits between devices Specifies voltage, wire speed and pin-out of cables	Physical topology

the ISO/OSI framework; therefore, there is no direct match between the TCP/IP standards and the layers of the framework.

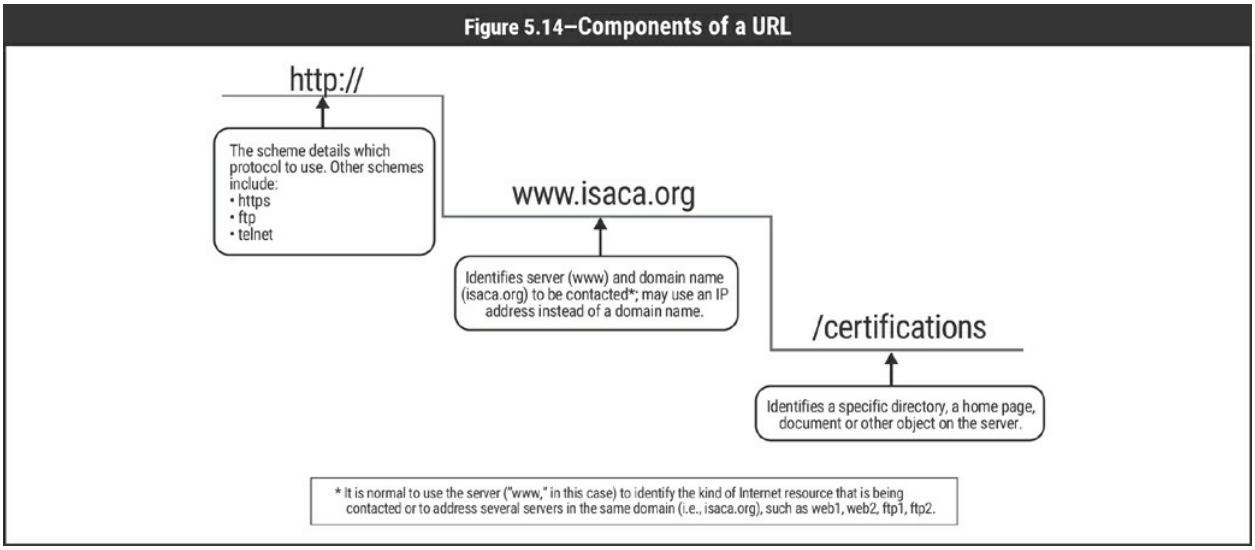
TCP/IP Internet World Wide Web Services

The most common way a user accesses a resource on the Internet is through the TCP/IP Internet World Wide Web (WWW) application service.

The uniform resource locator (URL) identifies the address on the WWW

where a specific resource is located. To access a website, a user enters the site's

location into their browser’s URL space, or they click on the hypertext



link that will send them to the location. The web browser looks up the IP

address of the site and sends a request for the URL via the HTTP. This protocol defines how the web browser and web server communicate with one another.

URLs contain several parts, as seen in **figure 5.14**.

A URL can also be used to access other TCP/IP Internet services, such as:

• *ftp://isaca.org*

• *telnet://isaca.org*

The URL is the location of specific resources (e.g., pages, data) or services on the Internet. In the example, the resource is a web page called

“certification” and is found on the web server of ISACA. This request is sent over the Internet and the routers transfer the request to the addressed web server, which activates the HTTP protocol and processes the request. When the server finds among its resources the requested home page, document or object, it sends the request back to the web browser. In the case of an HTML

page, the information sent back contains data and formatting specifications.

These are in the form of a program that is executed by the client web browser

and produce the screen displayed for the user. After the page is sent by the server, the HTTP connection is closed and can be reopened. **Figure 5.15**

displays the path.

Common gateway interface (CGI) scripts are an executable, machine-independent software program that is run on the server and can be called and executed by a web server. CGI scripts perform a specific set of tasks, such as processing input received from a client who typed information into a form on a web page. CGI scripts are coded in languages such as PERL or C. Note that CGI scripts need to be closely evaluated as they are run in the server; a bug in the scripts may allow a user to get unauthorized access to the server and, from there, eventually to the organization's network.

A **cookie** is a message stored by the web browser for the purpose of identifying users and possibly preparing customized web pages for them.

Depending on the browser, the implementation may vary, but the process is as follows. When entering, for the first time, a website that uses cookies, the user may be asked to go through a registration process, such as filling out a form that provides information, including name and interests. The web server will send back a cookie with information (text message in HTTP header), which will be kept as a text message by the browser. Afterward, whenever the user's browser requests a page from that particular server, the cookie's message is sent back to the server so that the customized view, based on that user's particular interests and preferences, can be produced. Cookies are a very important functionality because the HTTP protocol does not natively support the concept of a session. Cookies allow the web server to discern whether a known or new user is connected and to keep track of information previously sent to that user. The browser's implementation of cookies has, however, brought several privacy and security concerns, allowing breaches of security and the theft of personal information (e.g., user passwords that validate the user's identity and enable restricted web services).

Applets are programs written in a portable, platform-independent computer language, such as Java, JavaScript or Visual Basic. Applets expose the user's machine to risk if the applets are not properly controlled by the browser. For example, the user's browser should be configured to not allow an applet to access a machine's information without prior authorization of the user.

Servlets are Java applets or small programs that run within a web server environment. A Java servlet is similar to a CGI program. Unlike a CGI

program, once it is started, it stays in memory and can fulfill multiple requests, thereby saving server execution time and speeding up the services.

A **bookmark** is a marker or address that identifies a document or a specific place in a document.

General Internet Terminology

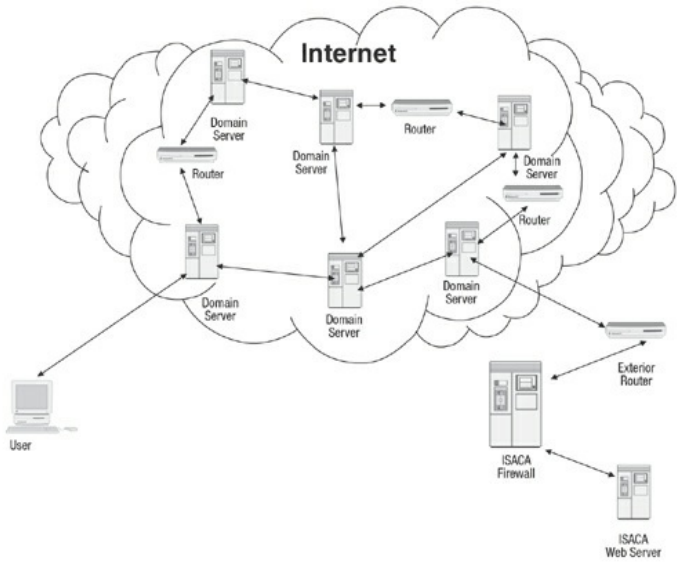
The following terms are related to the use of the Internet:

• **Direct connection**—LANs or large computers, such as mainframes, that can be directly connected to the Internet. When a LAN is connected to the Internet, all the computers on the network can have full access to the Internet.

• **Domain name system (DNS)**—A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services, such as web and email servers.

• **File Transfer Protocol (FTP)**—A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). These files can be of many types, including programs that the user can run on their computer—files with graphics, sounds and music, or text files that can be read. Most Internet files are downloaded using FTP. FTP can also be used to upload files from the computer to another computer on the Internet. To log onto an FTP site and download files, an account (or user name) and a password may need to be entered before the server or system allows the user to download or upload files. Some sites allow anyone to enter and download files. These sites are often referred to as anonymous FTP sites. As the definition suggests, anonymous FTP requires only a fictitious ID and password to transfer files. Anonymous FTP sites can be potentially dangerous if the network administrator setting up the site does not fully understand the risk associated with anonymous FTP. If file permissions have not been specified, the anonymous FTP user could also freely upload files to the server, introducing new files or changing existing files.

Figure 5.15—Internet Pathway Example



• **Internet link**—The connection between Internet users and the Internet service provider

• **ISP**—A third party that provides individuals and enterprises with access to the Internet and a variety of other Internet-related services.

• **Network Access Point (NAP)**—A traffic concentration spot, usually the point of convergence for Internet access by many Internet service providers

• **Online services**—All of the major online services allow users to tap the full power of the Internet. No special setup is required. When users dial into the online services, they are able to use the Internet resources, including browsing the World Wide Web.

• **Remote Terminal Control Protocol (Telnet)**—A standard terminal emulation protocol used for remote terminal connections, enabling users to log into remote systems and use resources as if they were local. An IS

auditor should note that standard Telnet traffic is not encrypted by default and consider this risk for any production Telnet use.

• **Secure Shell (SSH)**—Network protocol that uses cryptography to secure communication, remote command line login and remote command

execution between two networked computers

• **Simple Mail Transport Protocol (SMTP)**—The standard email protocol on the Internet

Transborder Data Flow

Transborder data flow refers to data transmission between two countries.

Information, such as email, invoices, payment advice, etc., can be transmitted via sub-oceanic cables, telephone, television links and satellites. The selection of transmission alternatives should consider cost and possible transmission delays. The country of origin or the country of destination could have several laws applicable to transborder data flow that should be addressed. Legal compliance and protection, as well as data security and integrity, are a concern with transborder transmissions. Privacy also is an issue because laws regarding protection and access to personal information may be different or conflicting between the source and destination countries.

Some countries also have laws concerning the encryption of data/information sent via transborder communications, thereby affecting the security and protection of data that may be exchanged between countries.

This is a particularly important issue in Internet communications, because the itinerary of the information is determined by the routers, is not fixed and, therefore, may cross a country border even while connecting two computers located in the same country.

Network Administration and Control

Network administration ensures that the network is functioning properly from a performance and security perspective. These duties include monitoring usage and throughput, load balancing, reacting to security violations and failure conditions, saving and restoring data, and making changes for scalability as the network usage grows. Therefore, an appropriate knowledge of network structure and topology, the protocols used, and the available administration tools is required.

The software used to monitor the network and enact changes should be accessible to the network administrator only. This software is the network OSs software associated with specific network devices, principally switches and routers.

The network OSs provide many functions aimed at shaping the network as a unified, controlled and uniform computing environment, including:

• Support local and remote terminal access to hosts and servers.

• Support sharing of common network resources, such as file and print services.

• Establish links to hosts and servers.

Network OSs have the following user-oriented features:

• Allow transparent access to the various resources of the network hosts.

• Check the user authorization to particular resources.

• Mediate and simplify the access to remote resources as easily as local resources.

• Establish uniform logon and logging procedures throughout the network.

• Make available up-to-the-minute online network documentation.

• Permit more reliable operation than possible on a single host or server, particularly when groups of equivalent hosts are used.

Network Performance Metrics

The major network performance metrics are latency and throughput. Network error counts and number of retransmissions are also measured to understand network performance.

• **Latency**—The delay that a message or packet will experience on its way from source to destination. Latency appears because the information needs to cross through different devices (switching and routing times) and, to a lesser extent, because signals must travel some distance (propagation delay). When a network device is busy, the packets either must wait, be queued in a buffer or be dropped. A very easy way to measure latency in a TCP/IP network is to use the ping command.

• **Throughput**—The quantity of useful work made by the system per unit of

time. In telecommunications, it is the number of bytes per second that are passing through a channel.

Network Management Issues

It is much more common today to see WANs communicating with a mix of LAN and host systems network architecture (SNA) traffic, or pure LAN-oriented traffic. Almost all organizations are standardizing their telecommunications, infrastructure on TCP/IP and modern routers.

This trend to a different technical design approach is also made evident by the specific name (i.e., WAN) that designates telecommunication networks in a TCP/IP environment. A WAN needs to be monitored and managed

similarly to a LAN. ISO, as part of its communications modeling effort (ISO/IEC 10040), has defined five basic tasks related to network management:

• **Fault management**—Detects the devices that present some kind of technical fault

• **Configuration management**—Allows users to know, define and change, remotely, the configuration of any device

• **Accounting resources**—Holds the records of the resource usage in the WAN (who uses what)

• **Performance management**—Monitors usage levels and sets alarms when a threshold has been surpassed

• **Security management**—Detects suspicious traffic or users, and generates alarms accordingly

Network Management Tools

In an organization’s modern internetworking environment, all of the previous tasks could be accomplished by a set of tools generically called network management tools.

Response time reports identify the time necessary for a command entered by a user at a terminal to be answered by the host system. Response time is important

because end users experiencing slow response time will be reluctant to use IS resources to their fullest extent. These reports typically identify average, worst and best response times over a given time interval for individual telecommunication lines or systems. These reports should be reviewed by IS management and system support personnel to track potential problems. If response time is slow, all possible causes, such as input/output (I/O) channel bottlenecks, bandwidth utilization and central processing unit (CPU) capacity, should be investigated; various solutions should be analyzed; and an appropriate and cost-justified corrective action should be taken.

Downtime reports track the availability of telecommunication lines and circuits. Interruptions due to power/line failure, traffic overload, operator

error or other anomalous conditions are identified in a downtime report. If downtime is excessive, IS management should consider the following remedies:

• Add or replace telecommunications lines.

• Switch to a more dependable transmission link (such as dedicated lines versus shared lines).

• Install backup power supplies.

• Improve access controls.

• Closely monitor line utilization to better forecast user needs, both in the near and long term.

Online monitors check data transmission accuracy and errors. Monitoring can be performed by echo checking (received data are bounced back to sender for verification) and status checking all transmissions, ensuring that messages are not lost or transmitted more than once.

Network monitors provide a real time display of network nodes and status.

Network (Protocol) analyzers are diagnostic tools attached to a network link that use network protocols' intelligence for monitoring the packets flowing along the link and produce network usage reports. Network analyzers are typically hardware-based and operate at the data link and/or network level.

Output includes the following information:

• Protocol(s) in use

• The type of packets flowing along the monitored link

• Traffic volume analysis

• Hardware errors, noise and software problems

• Other performance statistics (e.g., percentage of used bandwidth)

• Problems and possible solutions

Simple Network Management Protocol (SNMP) is a TCP/IP-based protocol that monitors and controls different variables throughout the network, manages configurations, and collects statistics on performance and security. A master console polls all the network devices on a regular basis and displays the global status. SNMP software is capable of accepting, in real-time, specific operator requests. Based on the operator instructions,

SNMP software sends specific commands to an SNMP-enabled device and retrieves the required information. To perform all of these tasks, each device (routers, switches, hubs, PCs, servers) needs to have a SNMP agent running.

The actual SNMP communications occur between all the agents and the console.

Help desk reports are prepared by the help desk, which is staffed or supported by IT technicians trained to handle problems occurring during normal IS usage. If an end user encounters any problem, he/she can contact the help desk for assistance. Help desk facilities are critical to the telecommunication environment since they provide end users with an easy means of identifying and resolving problems quickly, before they have a major impact on IS performance and end-user resource utilization. Reports prepared by the help desk provide a history of the problems and their resolution.

Applications in a Networked Environment

There are different types of applications used in a networked architecture.

Client-Server Technology

Client-server is a network architecture in which each computer or process on the network is either a server (a source of services and data) or a client (a user of these services and data that relies on servers to obtain them). In a client-server technology, the available computing power can be distributed and shared among the client workstations. Use of client-server technology is one of the most popular trends in building applications aimed at networked environments. Often, in a client-server network environment, the server provides data distribution and security functions to other computers that are independently running various applications.

The client-server architecture has a number of advantages, such as distributing the work among servers and performing as much computational work as possible on the client workstation to save bandwidth and server computing power. Important tasks, such as manipulating and changing data, may be performed locally and without the need for controlling resources on the main processing unit. In this way, the applications may run more

efficiently.

To achieve these advantages, client-server application systems are divided into separate pieces or tasks. The systems are split so that processing may take place on different machines (e.g., servers and clients). Each processing component is mutually dependent on the others. That tasks are performed on both client and server is the main difference between client-server processing and the traditional mainframe/distributed processing.

The typical client is a single PC or workstation. Presentation usually is provided by visually enhanced processing software, known as a graphical user interface (GUI). Clients may be thick or thin. A thin client (sometimes called a lean client) is a client computer or client software that depends primarily on the central server for processing activities and mainly focuses on conveying input and output between the user and the remote server. Many thin client devices run only web browsers or remote desktop software, meaning that all significant processing occurs on the server. In contrast, a thick or fat client does as much processing as possible and passes only data for communications and storage to the server.

The server is one or more multiuser computers. Server functions include any centrally supported role, such as file sharing, printer sharing, database access and management, communication services, email services, and processing application logic. Multiple functions may be supported by a single server.

Client-server architecture can be two-tiered which is normally composed of:

• A thick client, focused on GUI tasks and running the application logic

• A group (one or more) of database servers

The main disadvantages of this model are the requirement to keep the programs on the clients synchronized (ensuring that they are running the same logic) and its scalability.

Client-server architecture is more normally based on (at least) three levels of computing tasks (i.e., three-tier architectures). A three-tier architecture is composed of:

• A thin client, focused on GUI tasks (most often but not always web

browsers)

• A group (one or more) of application servers, focused on running the application logic

• A group (one or more) of database servers

This architecture does not have the limitations of two-tier applications and has other advantages, such as:

• Thin clients, which are less complex and less costly to buy and maintain

• More scalability (up to several thousands of concurrent users) because the load is balanced among different servers. This, in turn, improves overall system performance and reliability since more of the processing load can be accommodated simultaneously.

• Can be implemented in applications for internal usage only or in ebusiness applications (in this case, there could be another tier represented by the web

server)

• All of the program logic is separated from the rest of the code (via application servers)

Designs that contain more than two tiers are referred to as multitiered or n-tiered. N-tiered architecture applications are more complex to build and more difficult to maintain.

In an n-tiered environment, each instance of the client software can send data requests to one or more connected servers. In turn, the servers can accept these requests, process them and return the requested information to the client. This concept can be applied to many different kinds of applications the architecture remaining fundamentally the same. The interaction between client and server is often described using sequence diagrams. Sequence diagrams are standardized in the Unified Modeling Language.

Note: Implicit in n-tiered architectures is the presence of middleware that supports not just the communications between clients and servers, but the more advanced features, such as load balancing and fail over, dynamic location of components, and establishing synchronous connections or asynchronous queue-based messages

Middleware

Middleware is a client-server-specific term used to describe a unique class of software employed by client-server applications. Middleware serves as the glue between two otherwise distinct applications and provides services, such as identification, authentication, authorization, directories and security. This software resides between an application and the network and manages the interaction between the GUI on the front end and data servers on the back end. Middleware facilitates the client-server connections over the network and allows client applications to access and update remote databases and mainframe files.

Middleware is commonly used for:

• **Transaction processing (TP) monitors**—Programs that handle and monitor database transactions, and are used primarily for load balancing

• **Remote procedure calls (RPC)**—A protocol that enables a program on the

client computer to execute another program on a remote computer (usually a server)

• **Object request broker (ORB) technology**—The use of shared, reusable business objects in a distributed computing environment

– This provides the ability to support interoperability across languages and platforms, as well as enhance maintainability and adaptability of the system. Examples of such technologies are CORBA and Microsoft's

COM/DCOM.

• **Messaging servers**—Programs that asynchronously prioritize, queue and/or process messages using a dedicated server

Risk and controls associated with middleware in a client-server environment are:

• **Risk**—System integrity may be adversely affected because of the very purpose of middleware, which is intended to support multiple operating environments interacting concurrently. Lack of proper software to control portability of data or programs across multiple platforms could result in a loss of data or program integrity.

• **Controls**—Management should implement compensating controls to ensure the integrity of the client-server networks. Management should ensure that systems are properly tested and approved, modifications are

adequately authorized and implemented, and appropriate version control procedures are followed.

On-demand Computing

On-demand computing (ODC), also referred to as utility computing, is a computing model in which information system resources are allocated to users according to their current needs. The resources could be available within an organization or supplied by a third-party service provider. At any moment, a user (or organization) may need more bandwidth, CPU cycles, memory, application availability or other resource to a greater degree than another user. When that situation occurs, the resource can be made available to the user with the immediate need and taken away from the user with the lesser need.

A benefit of ODC is that an organization that is outsourcing its computing needs does not have to pay for excess computing capacity. A concern is the confidentiality of information maintained by the third-party provider.

5.5.8 NETWORK INFRASTRUCTURE SECURITY

Communication networks (i.e., WANs or LANs) generally include devices connected to the network as well as programs and files supporting the network operations. Control is accomplished through a network control terminal and specialized communications software.

The following are controls over the communication network:

• Network control functions should be performed by individuals possessing adequate training and experience.

• Network control functions should be separated, and the duties should be rotated on a regular basis, where possible.

• Network control software must restrict operator access from performing certain functions (e.g., the ability to amend/delete operator activity logs).

• Network control software should maintain an audit trail of all operator activities.

• Audit trails should be periodically reviewed by operations management to detect any unauthorized network operations activities.

• Network operation standards and protocols should be documented and

made available to the operators and should be reviewed periodically to ensure compliance.

• Network access by the system engineers should be monitored and reviewed closely to detect unauthorized access to the network.

• Analysis should be performed to ensure workload balance, fast response time and system efficiency.

• A terminal identification file should be maintained by the communications

software to check the authentication of a terminal when it tries to send or receive messages.

• Data encryption should be used, where appropriate, to protect messages from disclosure during transmission.

• Restrictions should be placed on remote printing facilities to ensure sensitive documents cannot be read by unauthorized personnel.

• Device hardening by keeping the devices up to date. That means upgrading the firmware, patching and updated to fix any security gaps.

To improve the control and maintenance of the infrastructure and its use, besides the direct management of the network devices, consolidate the logs of these devices with the firewall's logs and the client-server OS's logs.

In recent years, the management of large capacity storage units is frequently based on fiber channel connections.

Systems security is improved when a dynamic inventory of the devices is possible. In the case of an incident, it is important to know which computer is used by whom.

Another important security improvement is the ability to identify users at every step of their activity. Some application packages use predefined names (e.g., SYSTEM). New monitoring tools have been developed to resolve this problem.

Adopting an IT governance practice enables an organization to comply with network security requirements effectively. The Information Technology Infrastructure Library (ITIL) is a framework of practice guidance in information technology service management that can be used in setting up

SLAs, specifically for enterprise network operations, to maintain the uninterrupted operation of the network through controls, incident handling and auditing.

Client-server Security

A client-server is a network architecture in which each computer or process on the network is either a server (a source of services and data) or a client (a user of

these services and data that relies on servers to obtain them). Client-server architectures can be two-tiered (includes the use of a thick client), three-tiered (includes the use of application servers and a thin client, probably a browser) or n-tiered (includes multiple applications servers, middleware, etc.).

The security of a client-server environment is dependent on the security of its component parts. This includes the security of the:

• LAN

• Client

• OS

• Database

• Middleware

In a client-server environment, several access routes exist because application data may exist on the server or on the client. Therefore, each of these routes must be examined individually and in relation to each other to ensure that no exposures are left unchecked.

An additional risk to consider with the client-server model is the potential gaps among the components. In other words, how do the components connect to each other?

For example, in a two-tiered environment, the thick client must connect to the database. To achieve this, either (1) every user has a database account, in which case they may be able to bypass the client application (and hence the application controls) and connect directly to the database or (2) a proxy user (i.e., a single account that connects to the database on behalf of all others) is used, in which case the database password must be stored somewhere. This

might be stored insecurely or unencrypted.

In a client-server environment the IS auditor should ensure that:

• Application controls cannot be bypassed.

• Passwords are always encrypted.

• Access to configuration or initialization files is kept to a minimum.

• Access to configuration or initialization files is audited.

Internet Security Controls

To establish effective Internet security controls, an organization must develop controls within an information systems security framework from which Internet security controls can be implemented and supported. Generally, the process for establishing such a framework entails defining, through corporate policies and procedures, the rules the organization will follow to control Internet usage. For example, one set of rules should address appropriate use of Internet resources with rules that might reserve Internet privileges for those with a business need, define what information resources should be available for outside users, and define trusted and untrusted networks within and outside the organization. Another set of rules should address the classification of the sensitivity or criticality of corporate information resources. This will help to determine what information will be available for use on the Internet and the level of security to be used for corporate resources of a sensitive or critical nature on the Internet.

From an evaluation of these issues, an organization will be able to develop guidelines specific to its situations for defining the level of security controls related to the confidentiality, integrity and availability of information resources (i.e., business applications) on the Internet. For example, OS

security hardening guidelines can be developed that define how the OS

should be configured, detail which Internet services should be blocked from use or exploitation by external untrusted users and define how the system will be protected by firewalls. Additionally, supporting processes over these controls should be defined including:

• Risk assessments performed periodically over the development and redesign of Internet-based web applications

• Security awareness and training for employees, tailored to their levels of

responsibilities

• Firewall standards and security to develop and implement firewall architectures

• Intrusion detection standards and security to develop and implement IDS

architectures

• Remote access for coordinating and centrally controlling dial-up access on the Internet via corporate resources

• Incident handling and response for detection, response, containment and recovery

• Configuration management for controlling the security baseline when changes do occur

• Encryption techniques applied to protect information assets passing over the Internet

• A common desktop environment to control, in an automated fashion, what is displayed on a user's desktop

• Monitoring Internet activities for unauthorized usage and notification to end users of security incidents via computer emergency response team (CERT) bulletins or alerts

In summary, Internet usage is drastically changing the way business is done and is creating opportunities for organizations to compete in what has become a global virtual market. To compete and survive in this new marketplace, organizations have to go through a paradigm shift in the way they regard security. Security, as it relates to the Internet, will have to be considered an enabler for success and treated as an essential business tool.

Firewall Security Systems

Every time a corporation connects its internal computer network to the Internet, it faces potential danger. Because of the Internet's openness, every corporate network connected to it is vulnerable to attack. Hackers on the Internet could theoretically break into the corporate network and do harm in a number of ways

as described previously. Companies should build firewalls as one means of perimeter security for their networks. Likewise, this same principle holds true for sensitive or critical systems that need to be protected from untrusted users inside the corporate network (internal hackers).

Firewalls are defined as a device installed at the point where network

connections enter a site; they apply rules to control the type of networking traffic flowing in and out. Most commercial firewalls are built to handle the most commonly used Internet protocols.

To be effective, firewalls should allow individuals on the corporate network to access the Internet and, at the same time, stop hackers or others on the Internet from gaining access to the corporate network to cause damage.

Generally, most organizations will follow a deny-all philosophy, which means that access to a given resource will be denied unless a user can provide a specific business reason or need for access to the information resource. The converse of this access philosophy, not widely accepted, is the accept-all philosophy under which everyone is allowed access unless someone can provide a reason for denying access.

Firewall General Features

Firewalls are hardware and software combinations that are built using routers, servers and a variety of software. They separate networks from each other and screen the traffic between them. Thus, along with other types of security, they control the most vulnerable point between a corporate network and the Internet, and they can be as simple or complex as the corporate information security policy demands. There are many different types of firewalls, but most enable organizations to:

• Block access to particular sites on the Internet

• Limit traffic on an organization’s public services segment to relevant addresses and ports

• Prevent certain users from accessing certain servers or services

• Monitor communications and record communications between an internal and

an external network

• Monitor and record all communications between an internal network and the outside world to investigate network penetrations or detect internal subversion

• Encrypt packets that are sent between different physical locations within an organization by creating a VPN over the Internet (i.e., IPSec, VPN tunnels) The capabilities of some firewalls can be extended so they can also provide for protection against viruses and attacks directed to exploit known OS

vulnerabilities.

Firewall Types

Generally, the firewalls available today are associated with one of three categories:

• Packet filtering

• Application firewall systems

• Stateful inspection

Packet Filtering Firewalls

The simplest and earliest kinds of firewalls (i.e., first generation of firewalls) were packet filtering-based firewalls deployed between the private network and the Internet. In packet filtering, a screening router examines the header of every packet of data traveling between the Internet and the corporate network. Information contained in packet headers includes the IP address of the sender and receiver and the authorized port numbers (application or service) allowed to use the information transmitted. Based on that information, the router knows what kind of Internet service, such as web-based or FTP, is being used to send the data as well as the identities of the sender and receiver of the data. Using that information, the router can prevent certain packets from being sent between the Internet and the corporate network. For example, the router could block any traffic except for email or traffic to and from suspicious destinations.

The advantages of this type of firewall are its simplicity and generally stable performance as the filtering rules are performed at the network layer. Its

simplicity is also a disadvantage, because it is vulnerable to attacks from improperly configured filters and attacks tunneled over permitted services.

Because the direct exchange of packets is permitted between outside systems and inside systems, the potential for an attack is determined by the total number of hosts and services to which the packet filtering router permits traffic. Also, if a single packet filtering router is compromised, every system on the private network may be compromised and organizations with many routers may face difficulties in designing, coding and maintaining the rule base. This means that each host directly accessible from the Internet needs to support sophisticated user authentication and needs to be regularly examined

by the network administrator for signs of attack.

Some of the more common attacks against packet filter firewalls follow:

• **IP spoofing**—The attacker fakes the IP address of either an internal network host or a trusted network host so that the packet being sent will pass the rule base of the firewall. This allows for penetration of the system perimeter. If the spoofing uses an internal IP address, the firewall can be configured to drop the packet on the basis of packet flow direction analysis.

However, if the attacker has access to a secure or trusted external IP

address and spoofs on that address, the firewall architecture is defenseless.

• **Source routing specification**—It is possible to define the routing that an IP packet must take when it traverses from the source host to the destination host, across the Internet. In this process, it is possible to define the route, so it bypasses the firewall. Only those that know of the IP

address, subnet mask and default gateway settings at the firewall routing station can do this. A clear defense against this attack is to examine each packet and, if the source routing specification is enabled, drop that packet.

However, if the topology permits a route, skipping the choke point, this countermeasure will not be effective.

• **Miniature fragment attack**—Using this method, an attacker fragments the IP packet into smaller ones and pushes it through the firewall in the hope that only

the first of the sequence of fragmented packets would be examined and the others would pass without review. This is true if the default setting is to pass residual packets. This can be countered by configuring the firewall to drop all packets where IP fragmentation is enabled.

Application Firewall Systems

There are two types of application firewall systems—application-level and circuit-level firewall systems. They provide greater protection capabilities than packet filtering routers. Packet filtering routers allow the direct flow of packets between internal and external systems. Application and circuit gateway firewall systems allow information to flow between systems but do not allow the direct exchange of packets. The primary risk of allowing packet exchange between internal and external systems is that the host applications residing on the protected network's systems must be secure against any threat

posed by the allowed packets.

Application firewall systems could be an appliance or sit atop hardened (tightly secured) OSs, such as Windows or UNIX. They work at the application level of the OSI model. The application-level gateway firewall is a system that analyzes packets through a set of proxies—one for each service (e.g., HTTP proxy for web traffic, FTP proxy). An HTTP proxy is known as a web application firewall (WAF). This applies rules to HTTP conversations that cover known attacks, such as cross-site scripting (XSS) and Structured Query Language (SQL) injection. This kind of work could reduce network performance. Circuit-level firewalls are more efficient and also operate at the application level—where TCP and User Datagram Protocol (UDP) sessions are validated, typically through a single, general-purpose proxy before opening a connection. Commercially, circuit-level firewalls are quite rare.

Both application firewall systems employ the concept of bastion hosting in that they handle all incoming requests from the Internet to the corporate network, such as FTP or web requests. Bastion hosts are heavily fortified against attack. By having only a single host handling incoming requests, it is easier to maintain security and track attacks. Therefore, in the event of a break-in, only the firewall system has been compromised, not the entire network. In this way, none of the computers or hosts on the corporate network can be contacted directly for requests from the Internet, providing an effective level or layer of security.

Additionally, application-based firewall systems are set up as proxy servers to act on the behalf of someone inside an organization’s private network.

Rather than relying on a generic packet filtering tool to manage the flow of Internet services through the firewall, a special-purpose code called a proxy server is incorporated into the firewall system. For example, when someone inside the corporate network wants to access a server on the Internet, a request from the computer is sent to the proxy server, the proxy server contacts the server on the Internet, and the proxy server then sends the information from the Internet server to the computer inside the corporate network. By acting as a go-between, proxy servers can maintain security by examining a service’s (e.g., FTP, Telnet) program code and modifying and

securing it to eliminate known vulnerabilities. The proxy server can also log all traffic between the Internet and the network.

The application-level firewall implementation of proxy server functions is based on providing a separate proxy for each application service (e.g., FTP, Telnet and HTTP). This differs from circuit-level firewalls, which do not need a special proxy for each application-level service. In other words, one proxy server is used for all services.

Advantages of these types of firewalls are that they provide security for commonly used protocols and generally hide the internal network from outside untrusted networks. For example, a feature available on these types of firewall systems is the network address translation (NAT) capability. This capability takes private internal network addresses (unusable on the Internet) and maps them to a table of public IP addresses, assigned to the organization, which can be used across the Internet.

Disadvantages are poor performance and scalability as Internet usage grows.

To offset this problem, the concept of load balancing is applicable in cases where a redundant fail-over firewall system may be used.

Stateful Inspection Firewalls

A stateful inspection firewall keeps track of the destination IP address of each packet that leaves the organization’s internal network. Whenever the response to a packet is received, its record is referenced to ascertain and ensure that the

incoming message is in response to the request that went out from the organization. This is done by mapping the source IP address of an incoming packet with the list of destination IP addresses that is maintained and updated. This approach prevents any attack initiated and originated by an outsider.

The advantage of this approach over application firewall systems is that stateful inspection firewalls control the flow of IP traffic by matching information contained in the headers of connection-oriented or

connectionless IP packets at the transport layer, against a set of rules specified by the firewall administrator. This provides a greater degree of

efficiency when compared to typical CPU-intensive, full-time application firewall systems' proxy servers, which may perform extensive processing on each data packet at the application level.

A disadvantage of stateful inspection firewalls is that they can be relatively complex to administer, compared to the other two types of firewalls.

Examples of Firewall Implementations

Firewall implementations can take advantage of the functionality available in a variety of firewall designs to provide a robust layered approach in protecting an organization's information assets. Commonly used

implementations available today include:

• **Screened-host firewall**—Utilizing a packet-filtering router and a bastion host, this approach implements basic network layer security (packet filtering) and application server security (proxy services). An intruder in this configuration has to penetrate two separate systems before the security of the private network can be compromised. This firewall system is configured with the bastion host connected to the private network with a packet filtering router between the Internet and the bastion host. Router filtering rules allow inbound traffic to access only the bastion host, which blocks access to internal systems. Because the inside hosts reside on the same network as the bastion host, the security policy of the organization determines whether inside systems are permitted direct access to the Internet or whether they are required to use the proxy services on the bastion host.

• **Dual-homed firewall**—This is a firewall system that has two or more network interfaces, each of which is connected to a different network. In a firewall configuration, a dual-homed firewall usually acts to block or filter some or all of the traffic trying to pass between the networks. A dual-homed firewall system is a more restrictive form of a screened-host firewall system, in which a dual-homed bastion host is configured with one interface established for information servers and another for private network host computers.

• **Demilitarized zone (DMZ) or screened-subnet firewall**—Utilizing two packet-filtering routers and a bastion host, this approach creates the most secure firewall system because it supports network- and application-level

security while defining a separate DMZ network. The DMZ functions as a small, isolated network for an organization's public servers, bastion host information servers and modem pools. Typically, DMZs are configured to limit access from the Internet and the organization's private network.

Incoming traffic access is restricted into the DMZ network by the outside router and protects the organization against certain attacks by limiting the services available for use. Consequently, external systems can access only the bastion host (and its proxying service capabilities to internal systems) and possibly information servers in the DMZ. The inside router provides a second line of defense, managing DMZ access to the private network, while accepting only traffic originating from the bastion host. For outbound traffic, the inside router manages private network access to the DMZ

network. It permits internal systems to access only the bastion host and information servers in the DMZ. The filtering rules on the outside router require the use of proxy services by accepting only outbound traffic on the bastion host. The key benefits of this system are that an intruder must penetrate three separate devices, private network addresses are not disclosed to the Internet, and internal systems do not have direct access to the Internet.

Firewall Issues

Issues related to implementing firewalls include:

• A false sense of security may exist if management feels that no further security checks and controls are needed on the internal network (i.e., the majority of incidents are caused by insiders, who are not controlled by firewalls).

• The circumvention of firewalls through the use of modems may connect users directly to ISPs. Management should provide assurance that the use of modems when a firewall exists is strictly controlled or prohibited altogether.

• Misconfigured firewalls may allow unknown and dangerous services to pass through freely.

• What constitutes a firewall may be misunderstood (e.g., companies claiming to have a firewall merely have a screening router).

• Monitoring activities may not occur on a regular basis (i.e., log settings not appropriately applied and reviewed).

• Firewall policies may not be maintained regularly.

• Most firewalls operate at the network layer; therefore, they do not stop any application-based or input-based attacks. Examples of such attacks include SQL injection and buffer-overflow attacks. Newer-generation firewalls are able to inspect traffic at the application layer and stop some of these attacks.

Firewall Platforms

Firewalls may be implemented using hardware or software platforms. When implemented in hardware, it will provide good performance with minimal system overhead. Although hardware-based firewall platforms are faster, they are not as flexible or scalable as software-based firewalls. Software-based firewalls are generally slower with significant systems overhead; however, they are flexible with additional services. They may include content and virus checking, before traffic is passed to users. It is generally better to use appliances, rather than normal servers, for the firewall. Appliances are normally installed with hardened OSs. When server-based firewalls are used, OSs in servers are often vulnerable to attacks. When the attacks on OSs succeed, the firewall is compromised. Appliance-type firewalls are, generally, significantly faster to set up and recover.

Development and Authorization of Network Changes

Network configuration changes to update telecommunications lines, terminals, modems and other network devices should be authorized in writing by management and implemented in a timely manner. The IS auditor can test this

change control by:

• Sampling recent change requests, looking for appropriate authorization and matching the request to the actual network device

• Matching recent network changes, such as new telecommunication lines, to added terminals and authorized change requests

As an added control, the IS auditor should determine who can access the network change software. This access should be restricted to senior network administrators.

Specific development and change control procedures should be in place for

network components' hardware and software. Procedures should cover:

• Firewalls

• Routers

• Switches

• Application gateways

• DNS/network topology

• Client software

• Network management software

• Web server hardware and configuration

• Application software

• Web pages

Unauthorized Changes

One of the most important objectives of change control procedures is to prevent or detect unauthorized changes to software, configurations or parameters, and data. Unauthorized changes include any changes to software or

configurations/parameters that occur without conforming to change control procedures. They include situations where changes are made to software code without authorization, in addition to legitimate changes made in accordance with change control procedures.

Controls to prevent unauthorized changes to software and software configurations include the following:

• Ensure SoD among software development, software administration and computer operations.

• Restrict the software development team's access to the development environment only.

• Restrict access to the software source codes.

Controls to detect unauthorized changes to software include software code comparison utilities. Unauthorized changes to configurations/parameters can be detected through logging and monitoring system administrator activities.

Changes to data normally are controlled through the applications. Application access control mechanisms and built in application controls normally prevent unauthorized access to data. These controls can be circumvented by direct

access to data. For this reason, direct access to data (specifically "write" or

"change" access) should be restricted and monitored.

5.5.9 SHADOW IT

Shadow IT is an application, tool, service or system that is used within an organization to collaborate, develop software, share content, store and manipulate data or serve any number of other purposes without being reviewed, tested, approved, implemented or secured by the organization's IT

and/or information security functions, in accordance with written policies and procedures. Shadow IT can drive disruption and innovation, but also has the potential to expose an enterprise to significant risk. To manage the upside and downside of shadow IT, an organization must determine the need for controls, employ appropriate controls where necessary and understand that applying

controls is not a one-time activity. Where controls are needed, their implementation must be followed by regular assessment to ensure that they are still in place and operating effectively.

There are many controls that can address the threats related to shadow IT and a variety of approaches to their assessment. Many of these are unique to the type of business, the organization's size and its risk appetite. Typical controls include the following:

• Shadow IT policy—A shadow IT policy that aligns with business

objectives and support security requirements.

• IT department as a service-delivery organization—A culture that encourages and rewards the achievement of a strong and supportive relationship between the IT department and business units, with IT

functioning in a consultative way.

• IT budgeting and procurement—A requirement that the IT department review and approve all IT related purchases.

• IT system consolidation (where feasible)—Limiting the number of service providers, networks, platforms, devices and/or media used to store, process or transmit data and consolidating applications to facilitate data management and consolidation of environments (e.g. datacenters) and overall technology footprint.

• User access and administrative rights—User administration rights or data

access rights that are explicitly assigned. Unassigned users cannot freely install or adopt new applications.

• User education—A formal IT user education program targeted at personnel in all business units.

• User activity monitoring—Recording and monitoring user activity.

• User data exchange—Establishing strong end-point controls.

5.6 DATA CLASSIFICATION

Effective control requires a detailed inventory of information assets. Creating this list is the first step in classifying assets and determining the level of protection needed for each asset.

Information assets have varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources and establishing specific security rules for each class, it is possible to define the level of access controls that should be applied to each information asset. Classification of information assets reduces the risk and cost of over- or under-protecting information resources in linking security to business objectives because it helps to build and maintain a consistent perspective of the security requirements for information assets throughout the organization.

The information owner is responsible for the information and should decide on the appropriate classification, based on the organization's data classification and handling policy. Classifications should be simple, such as designations by differing degrees for sensitivity and criticality. End-user managers and security administrators can then use these classifications in their risk assessment process to assist with determining who should be able to access what, and the most appropriate level of such access. Most organizations use a classification scheme with three to five levels of sensitivity. The number of classification categories should take into consideration the size and nature of the organization and the fact that complex schemes may become too impractical to use.

Data classification is a major part of managing data as an asset. Data

classification as a control measure should define the:

• Importance of the information asset

• Information asset owner

• Process for granting access

• Person responsible for approving the access rights and access levels

• Extent and depth of security controls

Data classification must consider legal, regulatory, contractual and internal requirements for maintaining privacy, confidentiality, integrity and availability of information. Data classification is also useful to identify who should have access to the production data used to run the business versus those who are permitted to access test data and programs under development. For example, application programmers or system development programmers should not have access to production data or programs.

Adopting a classification scheme and assigning the information to one sensitivity level enables uniform treatment of data, through applying level-specific policies and procedures rather than addressing each type of information. It is highly difficult to follow information security policies if documents and media are not assigned to a sensitivity level and users are not instructed how to deal with each piece of information. If documents or media are not labeled according to a classification scheme, this is an indicator of a potential misuse of information. Users might reveal confidential information because they did not know that the requirements prohibited disclosure. Social engineering capitalizes on this kind of misunderstanding at the end user level.

An example of classification of information is shown in **figure 5.16**.

Figure 5.16—Classification of Information

Public

Company Brochures

Information

Private

Internal policies, procedures, normal business email messages, information controlled

Information

by legislation, etc.

Sensitive

Unpublished financials, company secrets, etc.

Information

5.7 DATA ENCRYPTION AND ENCRYPTION-RELATED

TECHNIQUES

Encryption is the process of converting a plaintext message into a secure-coded form of text, called ciphertext, which cannot be understood without converting it back via decryption (the reverse process) to plaintext.

Encryption is done via a mathematical function and a special

encryption/decryption password called the key.

Encryption generally is used to:

• Protect data in transit over networks from unauthorized interception and manipulation

• Protect information stored on computers from unauthorized viewing and manipulation

• Deter and detect accidental or intentional alterations of data

• Verify authenticity of a transaction or document

In many countries, encryption is subject to governmental laws and regulations.

Encryption is limited in that it cannot prevent the loss or modification of data.

The protection of the keys is of paramount concern when using encryption systems. Therefore, even if encryption is regarded as an essential form of access control that should be incorporated into an organization's overall security landscape, it requires a thorough understanding of how schemes work as misuse or misconfiguration may significantly undermine the protection that an organization believes is in place.

5.7.1 KEY ELEMENTS OF ENCRYPTION SYSTEMS

Key elements of encryption systems include:

• **Encryption algorithm**—A mathematically based function that encrypts/decrypts data

• **Encryption keys**—A piece of information that is used by the encryption algorithm to make the encryption or decryption process unique. Similar to passwords, a user needs to provide the correct key to access or decrypt a message. The wrong key will decipher the message into an unreadable form.

• **Key length**—A predetermined length for the key. The longer the key, the more difficult it is to compromise in a brute force attack.

Encryption schemes are susceptible to brute force attacks in which an attacker repeatedly tries to decrypt a piece of ciphertext using all the possible encryption keys until the correct one is found (i.e., brute forcing stops when the ciphertext does not decrypt to a non-sense message). Because the amount of time required to search for the correct key depends exponentially on its length, it is fundamental to choose the key adequately to ensure the overall security of encryption scheme.

Attacks can also be mounted against the robustness of the underlying mathematical algorithms to speed up the brute forcing process. Cryptanalysis is the science of finding such weaknesses. For example, an algorithm prone to a known-plaintext attack allows an attacker to discard a large portion of the possible decryption keys if samples of ciphertexts and corresponding plaintexts are available. In a variation of this attack, the attacker guesses parts of the

plaintext by leveraging on statistical properties of the encrypted data (e.g., spotting vowels or finding the word “the” in an English text).

The randomness of key generation is also a significant factor in the ability to compromise an encryption scheme. Common words or phrases significantly lessen the key space combinations required to search for the key, diminishing the strength of the encryption algorithm. Therefore, the capabilities of a 128-bit encryption algorithm are diminished when encrypting keys are based on passwords, and the passwords lack randomness. Therefore, it is important that effective password syntax rules are applied, and easily guessed passwords are prohibited.

There are two types of encryption schemes: symmetric and asymmetric.

Symmetric key systems use a unique key (usually referred to as the secret key) for both encryption and decryption. The key is known as bidirectional because it encrypts and decrypts and it must be shared out of band (i.e., via a secure, alternative method to the encrypted message). In **asymmetric key systems** the decryption key is different than the one used for encryption. The keys are unidirectional—they encrypt or decrypt—but are complementary. In

asymmetric key systems, the two parties (the sender and the recipient) are not expected to trust each other to keep the secret key. In asymmetric systems the encryption key is publicly disclosed while the decryption key is kept private (asymmetric systems are also known as public-key schemes).

Another important component of cryptographic protection schemes are hash functions. These functions transform a text of arbitrary length into one of fixed width called the digest or the hash of the input text (a basic example of a hash function is one that just truncates a text string after a fixed number of characters). To be used in cryptographic protection schemes, a hash function must be one-way (i.e., making it hard to find a piece of text that generates a given hash). Such functions can be used to augment encryption schemes with integrity and authenticity properties. Hashing algorithms are an accurate integrity check tool. The hash detects changes of even a single bit in a message. A hash algorithm will calculate a hash value from the entire input message. The output digest itself is a fixed length, so even though the input message can be of variable length, the output is always the same length. The length depends on the hash algorithm used. For example, MD5 generates a digest length of 128 bits;

SHA-1, a digest of 160 bits; and SHA-512, a digest of 512 bits.

The most common message digest algorithms were MD5 and SHA-1. Due to security considerations, the industry is transitioning to SHA-2. SHA-2has six hash functions available with varying message digest lengths. SHA-3 has also been announced by the National Institute for Standards and Technology (NIST) in the event a successful attack is developed against SHA-2.

Note: The IS auditor should be familiar with how a digital signature functions to protect data. The specific types of message digest algorithms are not tested on the CISA exam.

When senders want to send a message and ensure that it has not been altered, they can compute the digest of the message and send it along with the message to the receiver. When the receiver receives the message and its digest, he/she independently computes the digest of the received message and

ensures that the digest computed is the same as the digest sent with the message **(figure 5.17)**.

5.7.2 SYMMETRIC KEY CRYPTOGRAPHIC SYSTEMS

Symmetric key cryptographic systems **(figure 5.18)** are based on a symmetric encryption algorithm, which uses a secret key to encrypt the plaintext to the ciphertext and the same key to decrypt the ciphertext to the corresponding plaintext. In this case, the key is said to be symmetric because the encryption key is the same as the decryption key.

The most common symmetric key cryptographic system used to be the Data Encryption Standard (DES). DES is based on a public algorithm approved by NIST and employs keys of 56 bits (plus 8 bits used for parity checking). The bits in the plaintext are processed one 64-bit block at a time and, as such, DES belongs to the category of block-ciphers (as opposed to stream-ciphers, which encode one bit at a time).

DES was withdrawn by NIST because its entire key space can be brute forced by a moderately large computer system within a relatively short period of time. Extensions of DES (Triple DES or 3DES) were proposed to extend the DES standard while retaining backward compatibility (it applies the DES

cipher algorithm three times to each data block). In 2001, NIST replaced DES

with the Advanced Encryption Standard (AES), a public algorithm that supports keys from 128 bits to 256 bits in size. Another commonly used symmetric key algorithm is RC4, a stream-cipher often used in SSL/TLS

protocol sessions.

Figure 5.17— Verifying Message Integrity Using a Hash Function

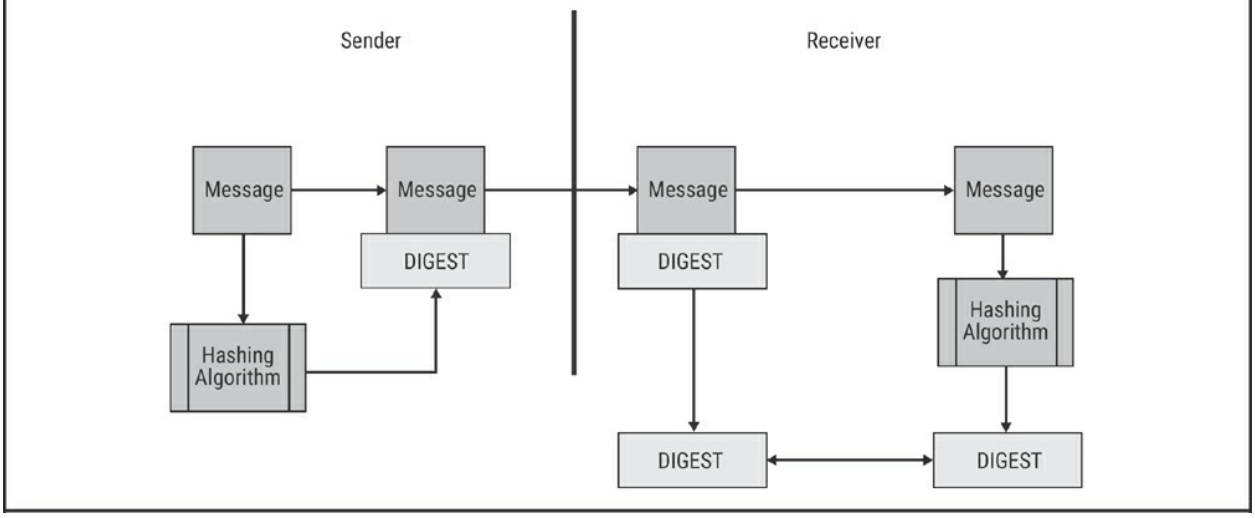
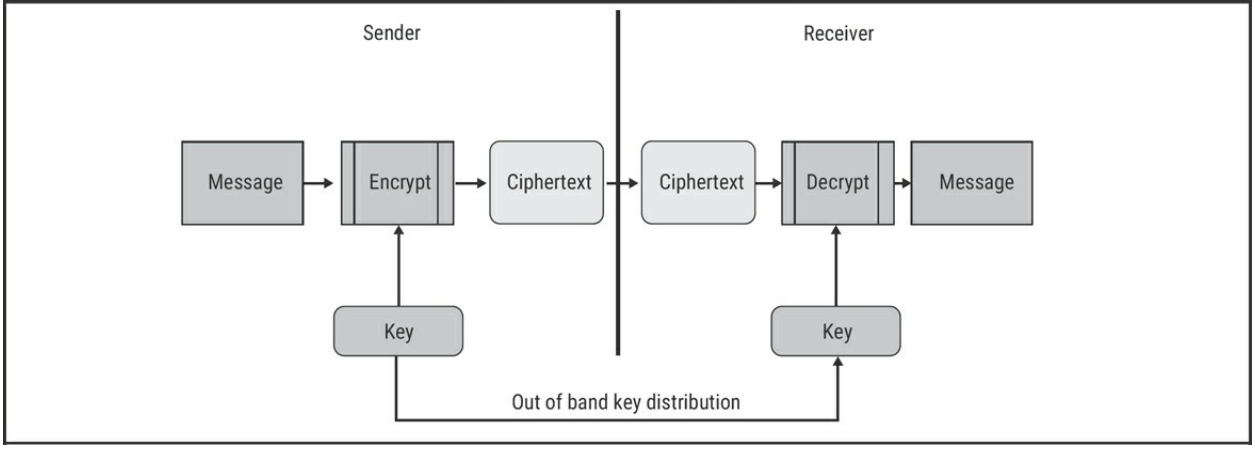


Figure 5.18—Symmetric Cryptography



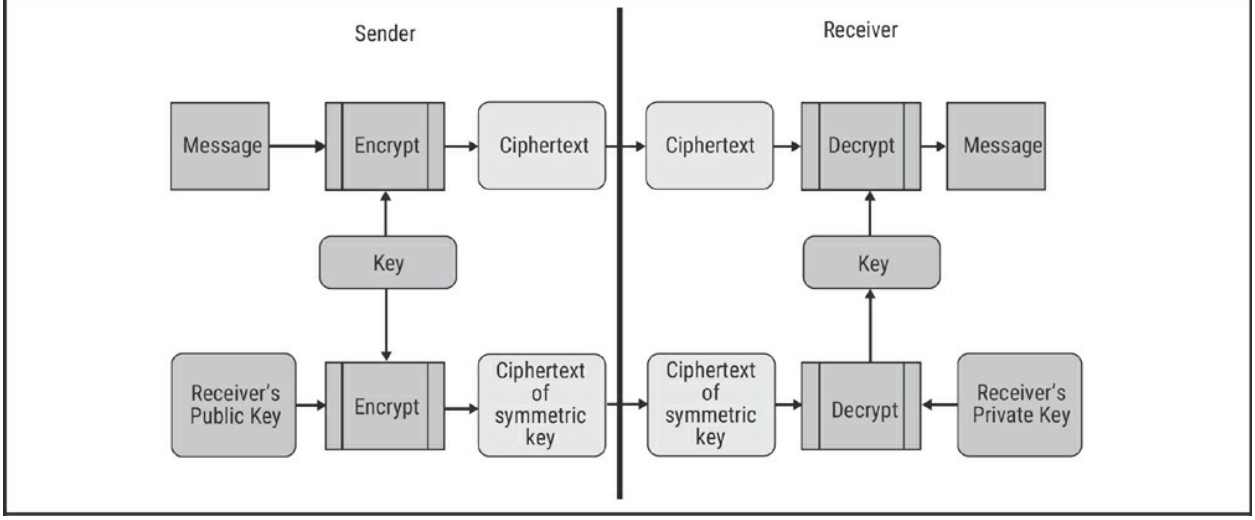
Source: ISACA, *CRISC Review Manual 6th Edition*, USA, 2015, figure 3.8

Source: ISACA, *CRISC Review Manual 6th Edition*, USA, 2015, figure 3.6

There are two main advantages symmetric key systems have over asymmetric ones. The first is that keys are much shorter and can be easily remembered.

The second is that symmetric key cryptosystems are generally less complicated and, therefore, use less processing power than asymmetric schemes. This makes symmetric key cryptosystems ideally suited for bulk data encryption. The major disadvantage of this approach is key distribution, particularly in ecommerce environments where customers are unknown, untrusted entities. Also, a symmetric key cannot be used to sign electronic documents or messages due to the fact that the mechanism is based on a shared secret by at least two parties.

Figure 5.19—Using Asymmetric Algorithms to Support Symmetric Cryptography



5.7.3 PUBLIC (ASYMMETRIC) KEY CRYPTOGRAPHIC SYSTEMS

In public key cryptography **(figure 5.19)**, two keys work together as a pair (they are inversely related to each other, based on mathematical integer factorization). One of the keys is kept private while the other one is publicly disclosed. Encryption works by feeding the public key to the underlying algorithm while the resulting ciphertext can be decoded using the private key.

This scheme avoids requirement of the owner of the key pair to share a secret piece of information (the private key) with the other party of the communication. It is important to note that one key pair can be used in one-direction only (from the sender to the receiver). To implement a bidirectional communication between two parties, two key-pairs are required (one for each direction).

Public key systems were developed primarily to solve the problem of key distribution. In the first place only 2*N key-pairs are employed in a scenario in

which communication happens between N parties: in the same scenario, a symmetric scheme would require roughly N^2 keys to be transmitted, one key for each pair of the involved parties. In addition, the exchanged keys are public, thus there is no confidentiality requirement to be fulfilled by the key distribution protocol.

Source: ISACA, *CRISC Review Manual 6th Edition*, USA, 2015, figure 3.7

The first practical implementation of a public key system was developed by Ron Rivest, Adi Shamir and Leonard Adleman (the RSA algorithm), which is a widespread asymmetric encryption scheme. The main drawback of this algorithm lies in the length of the keys (varying between 1024 and 4096 bits) and the complexity of the calculations involved for encoding and decoding.

To address these issues, other encryption algorithms were developed.

Promising alternatives like elliptic curve cryptography (ECC) are emerging because they have a much higher speed at encrypting/decrypting with significantly shorter keys (between 256 and 512 bits).

Quantum Cryptography

Quantum cryptography refers to the possibility of using properties of quantum computing (computer technology based on quantum theory) for cryptographic purposes, quantum key distribution (QKD) being the most important application. QKD schemes allow distribution of a shared encryption key between two parties who can detect when another

unauthorized party is eavesdropping on the key exchange channel. Indeed, when this happens, the channel is inevitably disturbed, and the exchanged key is tagged as compromised.

Quantum computing is also known to easily break the security of schemes like RSA. To overcome this drawback, postquantum encryption algorithms have been developed which are resistant to a quantum attack.

Digital Signatures

An important property of public key systems is that the underlying algorithm works even if the private key is used for encryption and the public key for

decryption. Even if this sounds counterintuitive, this way of using a public key system realizes a digital signature scheme able to authenticate the origin of an encoded message. Because the private key is known only by the owner of the key-pair, one can be sure that if a ciphertext is correctly decrypted using a public key, the owner of that public key cannot deny having performed the encryption process. This important and peculiar property of public key cryptosystems is called non-repudiation.

In most practical implementations of digital signature schemes **(figure 5.20)**,

the public key algorithm is never applied to the whole document as it would take a lot of processing power to calculate the signed data. Instead, a digest (or "pre-hash") is first derived from the document to be signed; then the public key algorithm is applied to the digest in order to produce an encoded piece of data (the signature) that is sent alongside the document.

To authenticate the sender as the originator of the document, the same hashing function is applied by the recipient upon receiving and the resulting digest (or post-hash) is compared with the decrypted pre-hash. In case of a match, the receiver can conclude that the document was actually signed by the owner of the public key.

Therefore, digital signature schemes ensure:

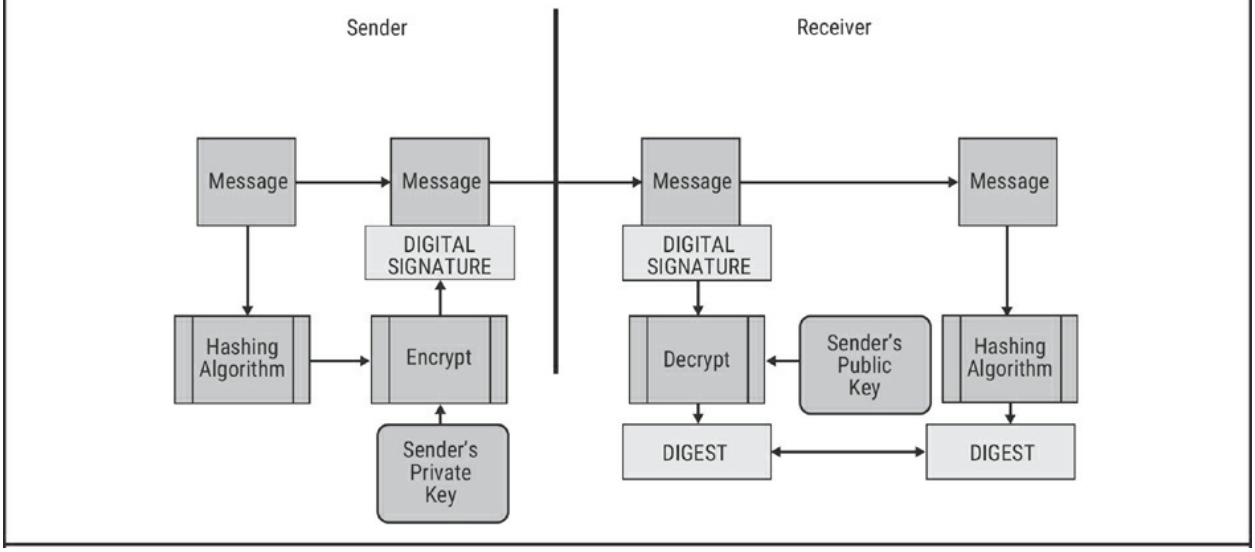
• **Data integrity**—Any change to the plaintext message would result in the recipient failing to compute the same document hash.

• **Authentication**—The recipient can ensure that the document has been sent by the claimed sender because only the claimed sender has the private key.

• **Nonrepudiation**—The claimed sender cannot later deny generating the document.

Notice that there is no guarantee that the owner of the public key actually sent the document. A malicious attacker could intercept the signed document and send it again to the recipient. To prevent this kind of attack (known as replay attack), a signed timestamping or a counter may be attached to the document.

Figure 5.20—Verifying Message Integrity and Proof of Origin Using Digital Signatures



Source: ISACA, *CRISC Review Manual 2015*, USA, 2014

Digital Envelope

Similar to a digital signature, a digital envelope is an electronic "container"

that can be used to protect data or a message through the use of encryption and data authentication. The message is first encoded using symmetric encryption and then the code to decode the message is secured using public key encryption. This provides a more convenient option for encryption.

5.7.4 APPLICATIONS OF CRYPTOGRAPHIC SYSTEMS

Asymmetric and symmetric systems can be combined together to leverage on each system's peculiarities. A common scheme is to encrypt data using a symmetric algorithm with a secret key, which is randomly generated. The secret key is then encrypted using an asymmetric encryption algorithm to allow the secure distribution among those parties who need access to the encrypted data. Secure communication can thus enjoy both the speed of symmetric systems and the ease of key-distribution of asymmetric systems.

In addition, because creating the secret key is an effortless operation, it can be employed just for a limited amount of data after which a new secret key can be chosen. This limits the possibilities of a malicious third-party to decrypt the whole set of data because he would be required to attack multiple secret keys.

This combined scheme is used in protocols, such as SSL/TLS, to protect web traffic and S/MIME for email encryption. In the latter case, the

resulting document—the combination of the encrypted message and the encrypted secret key—is called a digital envelope.

A more comprehensive list of applications of such a method follows.

Transport Layer Security

Transport layer security (TLS) is a cryptographic protocol that provides secure communications on the Internet. TLS is a session-or connection-layered protocol widely used for communication between browsers and web servers. Besides communication privacy, it also provides endpoint authentication. The protocols allow client-server applications to communicate in a way designed to prevent eavesdropping, tampering and message forgery.

TLS involves a few basic phases:

• Peer negotiation for algorithm support

• Public-key, encryption-based key exchange and certificate-based authentication

• Symmetric cipher-based traffic encryption

During the first phase, the client and server negotiate the cryptographic algorithms that will be used. Current implementations support the following choices:

• For public-key cryptography: RSA, Diffie-Hellman, DSA or Fortezza

• For symmetric ciphers: RC4, IDEA, Triple DES or AES

• For one-way hash functions: SHA-1 or SHA-2 (SHA-256)

TLS runs on layers above the TCP transport protocol and provides security to application protocols, even if it is most commonly used with HTTP to form Secure Hypertext Transmission Protocol (HTTPS). HTTPS serves to secure World Wide Web pages for applications. In electronic commerce,

authentication may be used in business-to-business (B-to-B) activities, in which the client and the server are authenticated, and business-to-consumer (B-to-C) interaction, in which only the server is authenticated.

Besides TLS, Secure Socket Layer (SSL) protocol is also widely used in real-world applications, even though its use is now deprecated as a significant

vulnerability was discovered in 2014. TLS and SSL are not interchangeable.

IP Security

IPSec is used for securing the communications at IP-level among two or more hosts, two or more subnets, or hosts and subnets.

This IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods. For the transport method, the data portion of each packet referred to as the encapsulation security payload (ESP) is encrypted, achieving confidentiality over the process. In the tunnel mode, the ESP payload and its header are encrypted. To achieve nonrepudiation, an additional authentication header (AH) is applied. In establishing IPSec sessions in either mode, security associations (SAs) are established. SAs define the security parameters that should be applied between the communicating parties as encryption algorithms, keys, initialization vectors, life span of keys, etc. Within either the ESP or AH header, respectively, an SA is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is a unique identifier that enables the sending host to reference the security parameters to apply, as specified, on the receiving host.

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes.

For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication and distribution of the SAs and those of the cryptographic keys.

Secure Shell

SSH is a client-server program that opens a secure, encrypted command-line

shell session from the Internet for remote logon. Similar to a VPN, SSH uses strong cryptography to protect data, including passwords, binary files and administrative commands, transmitted between systems on a network. SSH is typically implemented between two parties by validating each other's credentials via digital certificates. SSH is useful in replacing Telnet and is

implemented at the application layer, as opposed to operating at the network layer (IPSec implementation).

Secure Multipurpose Internet Mail Extensions (S/MIME)

S/MIME is a standard secure email protocol that authenticates the identity of the sender and receiver, verifies message integrity, and ensures the privacy of a message's contents, including attachments.

5.8 PUBLIC KEY INFRASTRUCTURE

Public key encryption algorithms are a big step toward strengthening the trust of secure communications, because private keys must not be shared by any of the parties involved in the system and no confidentiality requirements are imposed when distributing public keys.

However, public key systems are still vulnerable to man-in-the-middle (MITM) attacks in which the public keys are tampered with by an attacker (the man in the middle) controlling the communication channel. If this attacker replaces a genuine public key with his own key, any party sending a message to the owner of the tampered public key would instead be using the attacker's public key. This attacker is now able to intercept, read and modify any such message by decrypting and reencrypting it using the genuine public key. The problem lies in the fact that the tampering of the public key cannot be detected by either the sender or the recipient. In other words, there is no guarantee of a binding between the public key and the identity of the owner.

To solve this problem, a trusted third party is introduced into the scheme from which any signed document is considered automatically authentic by the sender and the recipient. In the first place, this trusted party identifies the holder of a public key (the subject) and then signs this public key while appending details of the subject's identity. The resulting document is known as the public (or digital) certificate of the subject. The trusted third party is called a certification authority (CA). When a CA is introduced in a signature scheme it is known as public key

infrastructure (PKI).

As well as issuing certificates, the CA maintains a list of compromised

certificates (i.e., those whose private key has been leaked or lost) called the certificate revocation list (CRL). In some cases, certificates may also be marked as revoked in the CRL when the owner of the certificate voluntarily declares not to use the corresponding key pair any longer. This allows a party to reject a signed document when the signature was generated after the private key has been compromised or revoked.

Certificates usually contain a certificate practice statement (CPS). This is a statement about the way a CA issues certificates.

It may contain:

• The type of certificates issued

• Policies, procedures and processes for issuing, renewing and recovering certificates

• Cryptographic algorithms used

• The key length used for the certificate

• The lifetime of the certificate issued by the CA

• Policies for revoking certificates

• Policies for CRLs

• Policies for renewing certificates

Registration authorities (RAs) are delegated some administrative functions for a specific community by the CA. For example, an international corporation may have a PKI setting in which national branches act as RAs for the employees in that nation.

The administrative functions that a particular RA implements will vary based on the needs of the CA but must support the principle of establishing or verifying

the identity of the subscriber. These functions may include the following:

• Verify information supplied by the subject (personal authentication functions).

• Verify the right of the subject to requested certificate attributes.

• Verify that the subject actually possesses the private key being registered and that it matches the public key requested for a certificate (generally referred to as proof of possession [POP]).

• Report key compromise or termination cases where revocation is required.

• Assign names for identification purposes.

• Generate shared secrets for use during the initialization and certificate pick-up phases of registration.

• Initiate the registration process with the CA on behalf of the subject end entity.

• Initiate the key recovery processing.

• Distribute the physical tokens (such as smart cards) containing the private keys.

5.9 WEB-BASED COMMUNICATION TECHNOLOGIES

The increasing complexity and convergence of voice and data

communications introduces additional risk that must be considered by the IS

auditor. Voice-over IP (VoIP) and public branch exchange (PBX)

environments involve security risk (both within and outside the enterprise) that must be addressed to ensure the security and reliability of voice communications. The IS auditor should have enough understanding of these concepts to establish the business risk and identify appropriate controls.

5.9.1 VOICE-OVER IP

IP telephony, also known as Internet telephony, is the technology that makes it possible to have a voice conversation over the Internet or over any dedicated IP network instead of dedicated voice transmission lines. The protocols used to

carry the signal over the IP network are commonly referred to as VoIP. VoIP is a technology where voice traffic is carried on top of existing data infrastructure. Sounds are digitized into IP packets and transferred through the network layer before being decoded back into the original voice. VoIP has significantly reduced long-distance costs in a number of large organizations.

VoIP allows the elimination of circuit switching and the associated waste of bandwidth. Instead, packet switching is used, where IP packets with voice data are sent over the network only when data needs to be sent.

It has advantages over traditional telephony:

• VoIP innovation progresses at market rates rather than at the rates of the multilateral committee process of the International Telecommunications Union (ITU)

• Lower costs per call or even free calls, especially for long-distance calls

• Lower infrastructure costs. Once IP infrastructure is installed, no or little additional telephony infrastructure is needed.

VoIP introduces security risk and opportunities. VoIP has a different architecture than traditional circuit-based telephony, and these differences result in significant security issues.

VoIP systems take a wide variety of forms, including traditional telephone handsets, conferencing units and mobile units. In addition to end-user equipment, VoIP systems include a variety of other components, including call processors/call managers, gateways, routers, firewalls and protocols.

Most of these components have counterparts used in data networks, but the performance demands of VoIP mean that ordinary network software and hardware must be supplemented with special VoIP components.

When designing a VoIP system, the backup has to be considered. While telecom companies usually operate under the requirement to have 99.9999

percent uptime, data traffic normally has less reliability. For this reason, the backup has to be designed to ensure that communication will not be interrupted should undesirable events occur on the data backbone. Bandwidth capacity

should be baselined to determine the current levels of data traffic and adjust the necessary additional bandwidth for voice traffic. Quality of service will need to be defined so that voice traffic will be given priority over data traffic. Other considerations are laws and regulations. Certain countries may ban the use of VoIP.

VoIP Security Issues

With the introduction of VoIP, the need for security is increased because two assets need to be protected—the data and the voice.

Protecting the security of conversations in VoIP is vital. In a conventional office telephone system, security is a more valid assumption. Intercepting

conversations requires physical access to telephone lines or compromise of the office private branch exchange (PBX). Only particularly security-sensitive organizations bother to encrypt voice traffic over traditional telephone lines. It cannot be said for Internet-based connections. In VoIP, packets are sent over the network from a user's computer or VoIP phone to similar equipment on the other end. Packets may pass through several intermediate systems that are not under the control of the user's ISP. The current Internet architecture does not provide the same physical wire security as the phone lines.

The dependence on VoIP communications implies a direct or indirect impact on:

• Communications, both within the enterprise and with the external world

• Ongoing business operations

• Customer relations

• Help desk and technical support

• Contractual issues

• Legal and compliance issues (e.g., risk of transmitting sensitive personal identifiable information (PII) in VoIP SMS messages or chat sessions, in breach of the US Health Insurance Portability and Accountability Act

[HIPAA] or PCI requirements)

Voice and multimedia communications typically contain or relate to business-critical information, including, but not limited to:

• Intellectual property (e.g., patents, copyrighted material)

• Sensitive corporate material, including data relating to financials, marketing and strategic planning, sensitive personnel information, sales and marketing, and daily business operations

• Communications with third parties, such as customers, government authorities, external legal counsel, joint venture partners, stockholders, stockbrokers and external auditors

• Audit work papers

• Issue monitoring

• Internal control documentation and testing

Failure to design and manage effective VoIP controls could result in:

• Destruction or loss of enterprise data due to penetration from unprotected VoIP networks

• Disclosure of sensitive information sent unencrypted across public networks

• Disclosure of sensitive information or related bad publicity, leading to reputational risk and loss of confidence by stakeholders, business partners, investors and customers

• Loss or theft of trade secrets and digital assets

• Theft of computing assets

• Loss of productivity due to unavailability of critical electronic assets, such as email, voice communications and instant messaging

• Fines and penalties, due to noncompliance or use of corporate VoIP

networks for undesirable activities, such as harassment, undesirable content and industrial espionage

• Security breaches due to malware carried by instant messaging

• Loss of sales due to inability of customers to reach sales personnel

• Brand damage and loss of competitive advantage

• Lawsuits by aggrieved third parties if hackers succeed in using compromised VoIP servers to attack other sites

• Inability to comply with legal discovery demands

• Inability to restore voice or multimedia communication within a reasonable time frame

• Officer liability

The key to securing VoIP is to use the security mechanisms, such as those deployed in data networks (e.g., firewalls, encryption) to emulate the security level currently used by public switched telephone network (PSTN) network users.

OS patches and virus signature updates must be promptly applied to prevent a potential system outage. To enhance the protection of the telephone system and data traffic, the VoIP infrastructure should be segregated using virtual local area networks (VLANs). Any connections between these two

infrastructures should be protected using firewalls that can interpret VoIP

protocols.

In many cases, session border controllers (SBCs) are used to provide security features for VoIP traffic similar to that provided by firewalls. SBCs can be configured to filter specific VoIP protocols, monitor for DoS attacks, and provide network address and protocol translation features.

5.9.2 PRIVATE BRANCH EXCHANGE

A PBX is a computer-based switch that can be thought of as essentially a small, in-house phone company for the organization that operates it.

Protection of the PBX is, thus, a high priority. Failure to secure a PBX can result in exposing the organization to toll fraud, theft of proprietary or confidential information, loss of revenue, or legal entanglements.

Although they are mostly being phased out, PBXs have been a part of organizations' communication infrastructures since the early 1920s, originally using analog technology. Current PBXs use digital signals converted to analog for outside calls using Plain Old Telephone Service (POTS), which refers to the standard telephone service that most homes formerly used.

One of the principal purposes of a PBX is to save the cost of requiring a line for each user to the telephone company's central office. Also, it is easier to call someone within a PBX because only three or four digits need to be dialed.

PBX Risk

Risk with using PBX includes:

• **Theft of service**—Toll fraud, probably the most common of motives for attackers

• **Disclosure of information**—Data disclosed without authorization, either by deliberate action or by accident. Examples include eavesdropping on conversations and unauthorized access to routing and address data.

• **Data modification**—Data altered in some meaningful way by reordering, deleting or modifying it. For example, an intruder may change billing information or modify system tables to gain additional services.

• **Unauthorized access**—Actions that permit an unauthorized user to gain access to system resources or privileges

• **Denial of service**—Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.

• **Traffic analysis**—A form of passive attack in which an intruder observes information about calls (although not necessarily the contents of the messages) and makes inferences (e.g., from the source and destination numbers or

frequency and length of the messages). For example, an intruder observes a high volume of calls between a company's legal department and patent office and concludes that a patent is being filed.

Although PBXs are computer systems and experience many threats that are similar to those experienced by an OS, they PBXs differ in two important ways:

• **External access/control**—Instead of relying on local administrators to make OS updates and patches, organizations normally have updates installed remotely by the switch manufacturer. This requires remote maintenance ports and access to the switch by a potentially large pool of outside parties.

• **Feature richness**—The variety of features available on PBXs, particularly administrative features and conference functions, provide the possibility of unexpected attacks.

PBX Audit

When planning a PBX audit, the type of skills, the number of auditors and the length of time required to perform the audit cannot be determined without a preliminary assessment of the PBX system, because these depend on the size and complexity of the chosen PBX. The type of perceived threat and the seriousness of any discovered vulnerabilities must be decided by the auditor.

Consequently, any corrective actions must also be determined based on the cost of the loss compared with the cost of the corrective action.

A list of critical items of PBX structure, usage and setup will be given, together with specific risk and applicable controls.

Protecting against all of the risk is not easy. Knowing that a given

vulnerability in fact exists is already a vital indication. A conservative approach of enabling only the needed features is advisable. Following are some controls to minimize PBX system attacks:

• Where possible, configure and secure separate and dedicated administrative ports.

• Control the definition of direct inward dialing (DID) lines to avoid an external

party requesting a dial tone locally, disabling that person’s ability to make unauthorized long-distance phone calls.

• Establish system access controls over long-distance phone calls (e.g., change default system vendor passwords, limit the 24/7 availability of PBX

lines).

• Block controls for long-distance phone calls to particular numbers (e.g., hot numbers, cellular numbers).

• Establish control over the numbers destined for fax machines and modems.

• Activate the option to register calls, enabling the use of call-tracking logs.

5.9.3 EMAIL SECURITY ISSUES

According to J. Klensin and the Network Working Group, when reading the engineering standards established for email, these documents clearly indicate the following:

• SMTP mail is inherently insecure; a low level of complexity and skill is needed to perform a man-in-the-middle attack between receiving and relaying SMTP servers to then spoof legitimate email traffic.

• Real mail security lies only in end-to-end methods involving the message bodies, such as those that use digital signatures or integrity checks provided, at the transport level.

Some other security issues involved in emails are as follows:

• Phishing and spear phishing are electronic social engineering attacks that have become exceedingly sophisticated and can only be addressed through security awareness training.

• Flaws in the configuration of the mail server application may be used as the means of compromising the underlying server and the attached network.

• DoS attacks may be directed to the mail server, denying or hindering valid users from using the mail server.

• Sensitive information transmitted unencrypted between mail server and email client may be intercepted.

• Information within the email may be altered at some point between the sender and recipient.

• Viruses and other types of malicious code may be distributed throughout an organization via email.

• Users may send inappropriate, proprietary or other sensitive information via email leading to a legal exposure.

To improve email security, organizations should:

• Address the security aspects of the deployment of a mail server through maintenance and administration standards

• Ensure that the mail server application is deployed, configured and managed to meet the security policy and guidelines instituted by management

• Consider the implementation of encryption technologies to protect user authentication and mail data

In the same way that authorizers in many organizations use email to communicate approvals for business transactions (e.g., payroll run, journal entry posting, payment authorization), it is important to adopt a calibrated approach for ensuring the authenticity of emails based on an informed risk assessment. For example, organizations may require emails communicating authorizations to be digitally signed by the sender before they can be acted on. In email security, a digital signature authenticates a transmission from a user in an untrusted network environment. A digital signature is a sequence of bits appended to a digital document. Like a handwritten signature, its authenticity can be verified. Unlike a handwritten signature, it is unique to the document being signed. Digital signatures are another application of public key cryptography. Digital signatures are a good method of securing email transmissions because:

• The signature cannot be forged.

• The signature is authentic and encrypted.

• The signature cannot be reused (a signature on one document cannot be transferred to another document).

• The signed document cannot be altered; any alteration to the document

(whether or not it has been encrypted) renders the signature invalid.

Email messages can be secured using either a symmetric key system using AES or with an asymmetric key system using pairs of unidirectional (only encrypt or decrypt), complementary keys. If the email transmission is secured with use of a symmetric key on the receiver's end, the user needs to know the single secret key to decrypt the message. If the transmission is secured with an asymmetric key system using a public key, the user at the receiving end needs to use the private key to decrypt the message, as well as a digital signature verification program to verify the signature. Digital signatures are based on a procedure called message digesting, which computes a short, fixed-length number called a digest for any message of any length. Several different messages may have the same digest, but it is extremely difficult to produce any of them from the digest. A message digest is a cryptographically strong, one-way hash function of the message. It is similar to a checksum in that it compactly represents the message and is used to detect changes in the message. The message digest authenticates the user's message in such a way that if it were altered, the message would be considered corrupted.

Organizations should employ their network infrastructure to protect their mail server(s) through appropriate use of firewalls, routers and IDSs.

5.9.4 PEER-TO-PEER COMPUTING

Peer-to-peer computing (P2P) computing is a distributed architecture where tasks or workloads are shared between peers. In P2P computing, there is no specific server to which one connects. For the most part, the connection is established between two peers—a connection between any two or more systems for a common interest. P2P networks are used almost exclusively for file sharing. Enterprises should strongly consider the risk against any perceived advantages before allowing access to P2P networks (**figure 5.21**).

5.9.5 INSTANT MESSAGING

Instant messaging (IM) is a communications service that enables a user to chat in

real time over a network on the Internet. It is a popular mechanism for collaborating and keeping in touch. One can connect with another user and

chat with prompt acknowledgment and response, rather than sending

numerous email messages. However, there is risk associated with IM (**figure 5.22**).

Figure 5.21—Risk of Peer-to-peer Computing

Threats and Vulnerabilities

Risk

Controls

Introduction of viruses and

• Data leakage/theft

• Ensure that antivirus and anti-

malware to the

• “Owned” systems (zombies)

malware controls are installed

organizational network

• System downtime

on all systems and updated

• Resources required to clean

daily.

systems

• Block P2P traffic.

• Prevent installation of P2P

clients.

• Establish or update policies

and standards.

• Develop and conduct

awareness training and

campaigns to inform

employees of the risk involved

with P2P computing.

Copyrighted content held on

• Regulatory sanctions and fines

• Block P2P traffic.

the enterprises network

• Adverse legal actions

• Prevent installation of P2P

• Licensing issues

clients.

• Reputational damage

• Establish or update policies

and standards.

• Develop and conduct awareness training and campaigns to inform employees of the risk involved with P2P computing.

Excessive use of P2P in the workplace

• Network utilization issues
• Productivity loss

• Restrict P2P usage.
• Establish or update policies and standards.
• Develop and conduct awareness training and campaigns to inform employees of the risk involved with P2P computing.

IP address exposure

• IP spoofing
• Traffic sniffing

• Block P2P traffic.

• Prevent installation of P2P

• Other IP-based attacks

clients.

• Establish or update policies

and standards.

• Network address translation.

Figure 5.22—Risk of Instant Messaging

Threats and

Risk

Controls

Vulnerabilities

Introduction of

• Data leakage/theft

• Ensure that antivirus and anti-

viruses and

• “Owned” systems (zombies)

malware controls are installed on all

malware to the

• System downtime

systems and updated daily.

organizational

• Resources required to clean systems

• Block IM traffic.

network

• Only allow an enclosed corporate IM

(especially

solution.

through

• Establish or update policies and

phishing)

standards.

• Develop and conduct awareness

training and campaigns to inform

employees of the risk involved with

IM.

Eavesdropping

• Data leakage/theft

• Encrypt IM traffic.

• Only allow an enclosed corporate IM

solution.

• Establish or update policies and

standards.

• Develop and conduct awareness

training and campaigns to inform

employees of the risk involved with

IM.

Excessive use

• Network utilization issues

• Restrict IM usage.

of IM in the

• Productivity loss

• Establish or update policies and

workplace

standards.

• Develop and conduct awareness

training and campaigns to inform

employees of the risk involved with

IM.

5.9.6 SOCIAL MEDIA

Social media technology involves the creation and dissemination of content through social networks using the Internet. The differences between traditional and social media are defined by the level of interaction and interactivity available to the consumer. For example, a viewer can watch the news on television with no interactive feedback mechanisms, while social media tools allow consumers to comment, discuss and even distribute the news. Use of social media has created highly effective communication platforms where any user,

virtually anywhere in the world, can freely create content and disseminate this information in real time to a global audience

ranging in size from a handful to literally millions.

There are many types of social media tools: blogs (e.g., WordPress), image and video sharing sites (e.g., Flickr and YouTube), social networking (e.g., Facebook), and professional networking (e.g., LinkedIn). The common link among all forms of social media is that the content is supplied and managed by individual users who leverage the tools and platforms provided by social media sites.

Enterprises are using social media to increase brand recognition, sales, revenue and customer satisfaction; however, there is risk associated with its usage. These are divided into enterprises with a corporate social media presence (**figure 5.23**) and those whose employees engage in social media

(figure 5.24). Organizations should ensure that new and existing social media programs adhere to enterprise strategy, governance and management objectives and policies. The social media program should also ensure that the organization's brand is protected from negative publicity or other adverse issues to its reputation due to the use of social media.

Figure 5.23—Risk of a Corporate Social Media Presence

Threats and

Risk

Controls

Vulnerabilities

Introduction of

• Data leakage/theft

• Ensure that antivirus and anti-

viruses and

• “Owned” systems (zombies)

malware controls are installed on all

malware to the

• System downtime

systems and updated daily.

organizational

• Resources required to clean systems

• Use content filtering technology to

network

restrict or limit access to social media

sites.

• Ensure that appropriate controls are

also installed on mobile devices such

as smartphones.

• Establish or update policies and

standards.

• Develop and conduct awareness

training and campaigns to inform

employees of the risk involved with

using social media sites.

Exposure to

• Customer backlash/adverse legal

• Engage a brand protection firm that

customers and

actions

can scan the Internet and search out

the enterprise

• Exposure of customer information

misuse of the enterprise brand.

through a

• Reputational damage

• Give periodic informational updates

fraudulent or

• Targeted phishing attacks on

to customers to maintain awareness

hijacked

customers or employees

of potential fraud and to establish

corporate

clear guidelines regarding what

presence

information should be posted as part

of the enterprise social media

presence.

Unclear or

• Enterprise’s loss of control/legal

• Ensure that legal and

undefined

rights of information posted to the

communications teams carefully

content rights to

social media sites

review user agreements for social

information

media sites that are being considered.

posted to social

• Establish clear policies that dictate to

media sites

employees and customers what

information should be posted as part

of the enterprise social media

presence.

• If feasible and appropriate, ensure

that there is a capability to capture

and log all communications.

A move to a

• Customer dissatisfaction with the

• Ensure that staffing is adequate to

digital business

responsiveness received in this arena,

handle the amount of traffic that

model may

leading to potential reputational

could be created from a social media

increase

damage for the enterprise and

presence.

customer

customer retention issues

• Create notices that provide clear

service

windows for customer response.

expectations.

Mismanagement

• Regulatory sanctions and fines

• Establish appropriate policies,

of electronic

• Adverse legal actions

processes and technologies to ensure

communications

that communications via social media

that may be

that may be impacted by litigation or

impacted by

regulations are tracked and archived

retention

appropriately.

regulations or

• Note that, depending on the social

ediscovery

media site, maintaining an archive

may not be a recommended

approach.

Source: ISACA, *Social Media: Business Benefits and Security, Governance and Assurance Perspectives*, USA, 2010, figure 1

Figure 5.24—Risk of Employee Personal Use of Social Media

Threats and

Risk

Controls

Vulnerabilities

Use of

• Privacy violations

• Work with the human resources (HR)

personal

• Reputational damage

department to establish new policies

accounts to

• Loss of competitive advantage

or ensure that existing policies

communicate

address employee posting of work-

work-related

related information.

information

• Work with the HR department to

develop awareness training and

campaigns that reinforce these

policies.

Employee

• Brand damage

• Work with the HR department to

posting of

• Reputational damage

develop a policy that specifies how

pictures or

employees may use enterprise related

information

images, assets and intellectual

that link them

property (IP) in their online presence.

to the

enterprise

Excessive

• Network utilization issues

• Manage accessibility to social media

employee use

• Productivity loss

sites through content filtering or by

of social

• Increased risk of exposure to viruses

limiting network throughput to social

media in the

and malware due to longer duration of

media sites.

workplace

sessions

Employee

• Infection of mobile devices

• If possible, route enterprise

access to

• Data theft from mobile devices

smartphones through corporate

social media

• Circumvention of enterprise controls

network filtering technology to

via enterprise-

• Data leakage

restrict or limit access to social media

supplied

sites.

mobile devices

• Ensure that appropriate controls are

(smartphones,

also installed and continuously

tablets)

updated on mobile devices such as

smartphones.

• Establish or update policies and

standards regarding the use of

smartphones to access social media.

• Develop and conduct awareness

training and campaigns to inform

employees of the risk involved with

using social media sites.

Source: ISACA, *Social Media: Business Benefits and Security, Governance and Assurance Perspectives*, USA, 2010, figure 2

5.9.7 CLOUD COMPUTING

One issue surrounding the cloud and its related services is the lack of agreed-on definitions. For nearly all technologies, the lack of clarity and agreement often hinders the overall evaluation and adoption of that technology. Two groups that have offered a baseline of definitions are the National Institute of Standards and

Technology (NIST) and the Cloud Security Alliance® (CSA).

They both define cloud computing as a model for enabling convenient, on-

demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Another way to describe services offered in the cloud is to liken them to that of a utility. Just as enterprises pay for the electricity, gas and water they use, they now have the option of paying for IT services on a consumption basis.

The cloud model has three service models (**figure 5.25**), four deployment models **(figure 5.26)** and five essential characteristics **(figure 5.27)**. Overall risk and benefits will differ per model, and it is important to note that when considering different types of service and deployment models, enterprises should consider the risk that accompanies them.

Regardless of the models deployed, the security objectives required to meet an organization's business requirements must still be met. These include:

• Ensure the continued availability of their information systems and data.

• Ensure the integrity and preserve the confidentiality information and sensitive data while stored and in transit.

• Ensure conformity to applicable laws, regulations and standards.

• Ensure adherence to trust and obligation requirements in relation to any information relating to an identified or identifiable individual (i.e., data subject) in accordance with its privacy policy or applicable privacy laws and regulations.

Risk associated with cloud computing and associated controls is described in

figure 5.28.

Considerations for the IS auditor regarding cloud computing include:

• Data ownership, data custody and security administration related to cloud deployment models: The CSA provides a questionnaire that organizations can

use to ascertain a service providers compliance to the Controls Matrix.

• Legal requirements and unique risk in the cloud environment: Regulations, such as GDPR can present unique challenges for data stored in the cloud.

• Potential limitations to the right-to-audit in a cloud environment: An auditor may not be able to physically investigate a vendor’s facilities.

Figure 5.25—Cloud Computing Service Models

Service

Definition

To Be Considered

Model

Infrastructure

Capability to provision processing,

Options to minimize the impact if the

as a Service

storage, networks and other fundamental

cloud provider has a service interruption

(IaaS)

computing resources, offering the

customer the ability to deploy and run

arbitrary software, which can include

operating systems and applications. IaaS

puts these IT operations into the hands of

a third party.

Platform as a

Capability to deploy onto the cloud

• Availability

Service

infrastructure customer-created or

• Confidentiality

(PaaS)

acquired applications created using

• Privacy and legal liability in the event

programming languages and tools

of a security breach (as databases

supported by the provider

housing sensitive information will now

be hosted offsite)

• Data ownership

• Concerns around ediscovery

Software as a

Capability to use the provider’s

• Who owns the applications?

Service

applications running on cloud

• Where do the applications reside?

(SaaS)

infrastructure. The applications are

accessible from various client devices

through a thin client interface such as a

web browser (e.g., web-based email).

ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*,

USA, 2009, figure 1, page 5, *www.isaca.org/Knowledge-*

Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-

Governance-and-Assurance-Perspective.aspx

Figure 5.26—Cloud Computing Deployment Models

Deployment

Description of Cloud Infrastructure

To Be Considered

Model

Private

• Operated solely for an organization

• Cloud services with minimum risk

cloud

• May be managed by the organization or

• May not provide the scalability and

a third party

agility of public cloud services

• May exist on-premise or off-premise

Community

• Shared by several organizations

• Same as private cloud, plus:

cloud

• Supports a specific community that has

• Data may be stored with the data of

shared mission or interest.

competitors.

• May be managed by the organizations

or a third party

• May reside on-premise or off-premise

Public

• Made available to the general public or

• Same as community cloud, plus:

cloud

a large industry group

• Data may be stored in unknown

• Owned by an organization selling

locations and may not be easily

cloud services

retrievable.

Hybrid

A composition of two or more clouds

• Aggregate risk of merging different

cloud

(private, community or public) that

deployment models

remain unique entities but are bound

• Classification and labeling of data will

together by standardized or proprietary

be beneficial to the security manager to

technology that enables data and

ensure that data are assigned to the

application portability (e.g., cloud

correct cloud type.

bursting for load balancing between

clouds)

ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*,

USA, 2009, figure 2, page 5, *www.isaca.org/Knowledge-*

Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-

Governance-and-Assurance-Perspective.aspx

Figure 5.27—Cloud Computing Essential Characteristics

Characteristic

Definition

On-demand self-service

The cloud provider should have the ability to automatically provision computing capabilities, such as server and network storage, as needed without requiring human interaction with each service's provider.

Broad network access

According to NIST, the cloud network should be accessible

anywhere, by almost any device (e.g., smart phone, laptop, mobile devices).

Resource pooling

The provider's computing resources are pooled to serve multiple

customers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand. There is a sense of location independence. The customer

generally has no control or knowledge over the exact location of the provided resources. However, he/she may be able to specify location at a higher level of abstraction (e.g., country, region or data center).

Examples of resources include storage, processing, memory, network bandwidth

and virtual machines.

Rapid elasticity

Capabilities can be rapidly and elastically provisioned, in many cases automatically, to scale out quickly and rapidly released to scale in quickly. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored,

controlled and reported, providing transparency for both the provider

and customer of the utilized service.

ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*,

USA, 2009, figure 3, page 6, *www.isaca.org/Knowledge-*

Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-

Governance-and-Assurance-Perspective.aspx

Figure 5.28—Risk Associated with Cloud Computing

Risk

Description

Control

Legal

Cloud service providers (CSPs) are often

• Request the CSP’s list of infrastructure

transborder

transborder, and different countries have

locations and verify that regulation in

requirements

different legal requirements, especially

those locations is aligned with the

concerning personal private information.

enterprise’s requirements.

The enterprise might be committing a

• Include terms in the contract to restrict

violation of regulations in other

the moving of enterprise assets to only

countries when storing, processing or

those areas known to be compliant

transmitting data within the CSP’s

with the enterprise’s own regulation.

infrastructure without the necessary

• Prevent disclosure, encrypt any asset

compliance controls. Furthermore,

prior to migration to the CSP and

government entities in the hosting

ensure proper key management is in

country may require access to the

place.

enterprise’s information with or without

proper notification.

Physical

Physical security is required in any

• Request the CSP’s physical security

security

infrastructure. When the enterprise

policy and ensure that it is aligned

moves assets to a cloud infrastructure,

with the enterprise’s security policy.

those assets are still subject to the

• Request that the CSP provide proof of

corporate security policy, but they can

independent security reviews or

also be physically accessed by the CSP’s

certification reports that meet the

staff, which is subject to the CSP’s

enterprise’s compliance requirements
security policy. There could be a gap
(e.g., SOC reports, SOX, PCI DSS,
between the security measures provided
HIPAA, ISO certification).
by the CSP and the requirements of the
• Include in the contract language that
enterprise.
requires the CSP to be aligned with the
enterprise’s security policy and to
implement necessary controls to
ensure it.
• Request the CSP’s disaster recovery
plans and ensure that they contain the
necessary countermeasures to protect
physical assets during and after a
disaster.
Data disposal
Proper disposal of data is imperative to
• Request CSP’s technical specifications
prevent unauthorized disclosure. If

and controls that ensure that data are

appropriate measures are not taken by

properly wiped and backup media are

the CSP, information assets could be

destroyed when requested.

sent (without approval) to countries

• Include terms in the contract that

where the data can be legally disclosed

require, upon contract expiration or

due to different regulations concerning

any event ending the contract, a

sensitive data. Disks could be replaced,

mandatory data wipe carried out under

recycled or upgraded without proper

the enterprise’s supervision.

cleaning so that the information still

remains within storage and can later be

retrieved. When a contract expires, CSPs

should ensure the safe disposal or

destruction of any previous backups.

Any of the data fed into the CSP’s

application must be erased immediately using the necessary tools to avoid disclosures and confidentiality breaches (forensic cleaning may be required for sensitive data).

Multi-tenancy

One of the primary benefits of the cloud

• Request the CSP’s technical details for

and isolation

is the ability to perform dynamic approval and require additional

failure

allocation of physical resources when controls to ensure data privacy, when required. The most common approach is necessary.

a multi-tenant environment (public

• A contractual agreement is necessary

cloud), where different entities share a to officially clarify who is allowed to pool of resources, including storage,

access the enterprise’s information,
hardware and network components. For
naming specific roles for CSP
example, when allocated storage is no
employees and external partners. All
longer needed by a client it can be freely
controls protecting the enterprise’s
reallocated to another enterprise. In that
information assets must be clearly
case, sensitive data could be disclosed if
documented in the contract agreement
the storage has not been scrubbed
or service level agreement (SLA).
thoroughly (e.g., using forensic
• Use a private cloud deployment model
software). Furthermore, malicious
(no multi-tenancy).
entities in the cloud could take
advantage of shared information—for
example, by utilizing shared routing
tables to map the internal network

topology of an enterprise, preparing the

way for an internal attack.

Application

When applications are developed in a

• Include terms in the contract that

disposal

PaaS environment, originals and

require the proper disposal of

backups should always be available. In

applications including objects, source

the event of a contract termination, the

and backups.

details of the application could be

• Include non-compete clauses in the

disclosed and used to create more

contract.

selective attacks on applications or could

be copied violating the enterprise’s IP.

Lack of

Enterprises that use cloud applications

• If possible include a right of audit in

visibility into

have little visibility into the software

the contract.

software

SDLC. Customers do not know in detail

• Include in the contract language that

systems

how the applications were developed

requires the CSP to be aligned with the

development

and what security considerations were

enterprise’s security policy and to

life cycle

taken into account during the SDLC.

implement necessary controls to

(SDLC)

This could lead to an imbalance between

ensure it.

the security provided by the application

• Require SLAs that include a schedule

and the security required by

of software changes.

customers/users.

Lack of

CSPs are able to introduce patches in

• If possible, include a right of audit in

control of the

their applications quickly. These

the contract.

release

deployments are often done without the

• Include in the contract language that

management

approval (or even the knowledge) of the

requires the CSP to be aligned with the

process

application users for practical reasons: if

enterprise’s security policy and to

an application is used by hundreds of

implement necessary controls to

different enterprises, it would take an

ensure it.

extremely long time for a CSP to look

• Require SLAs that include a schedule

for the formal approval of every

of patches and software releases.

customer. In this case, the enterprise

could have no control (or no view) of

the release management process and

could be subject to unexpected side

effects.

Identity and

Information assets could be accessed by

• If possible, include a right of audit in

access

unauthorized entities due to faulty or

the contract.

management

vulnerable access management measures

• Include in the contract language that

(IAM)

or processes. This could result from a

requires the CSP to be aligned with the

forgery/theft of legitimate credentials or

enterprise’s security policy and to

a common technical practice (e.g.,

implement necessary controls to

administrator permissions override).

ensure it.

• Request that the CSP provide proof of

independent security reviews or

certification reports that meet the

enterprise’s compliance requirements

(e.g., SOC reports, SOX, PCI DSS,

HIPAA, ISO certification).

Service

Security for SOA presents new

• If possible include a right of audit in

Orientated

challenges because vulnerabilities arise

the contract.

Architecture

not only from the individual elements,

• Include in the contract language that

(SOA)–

but also from their mutual interaction.

requires the CSP to be aligned with the

related

Because the SOA libraries are under the

enterprise’s security policy and to

vulnerabilities

responsibility of the CSP and are not

implement necessary controls to

completely visible to the enterprise,

ensure it.

there may be unnoticed application

• Request that the CSP provide proof of

vulnerabilities.

independent security reviews or

certification reports that meet the

enterprise’s compliance requirements

(e.g., SOC reports, SOX, PCI DSS,

HIPAA, ISO certification).

Exit strategy

CSPs tools facilitate bring data to the

• Ensure by contract or SLA with the

cloud or CSP but rarely the other way

CSP an exit strategy that specifies the

around. This can make it very difficult

terms that should trigger the retrieval

for the enterprise to migrate from one

of the enterprise’s assets in the time

CSP to another or to bring services back

frame required by the enterprise.

in-house. It can also result in serious

• Implement a disaster recovery plan, business disruption or failure should the taking into account the possibility of CSP go bankrupt, face legal action or be complete CSP disruption.

the potential target for an acquisition (with the likelihood of sudden changes in CSP policies and any agreements in place). If the organization decides to bring the data back in-house, the question of how to securely render the data becomes critical because the in-house applications may have been decommissioned or “sunsetted” and there is no application available to render the data. Another possibility is the “run on the banks” scenario, in which there is a crisis of confidence in the CSP’s financial position resulting in a mass exit and withdrawal on first-

come, first-served basis. If there are limits to the amount of content that can be withdrawn in a given time frame, then the enterprise might not be able to retrieve all its data in the time specified.

Ease to

Business organizations may contract

• Require that the purchase of cloud

contract SaaS

cloud applications without proper

services follow the established

procurement and approval oversight,

procedures. Ensure executive

thus bypassing compliance with internal

management support for this.

enterprise policies.

Collateral

If one tenant of a public cloud is

• Ask the CSP to include the enterprise

damage

attacked, there could be an impact to the

in its incident management process

other tenants of the same CSP, even if

that deals with notification of

they are not the intended target (e.g.,

collateral events.

DDoS). Another possible scenario of

• Include contract clauses and controls

collateral damage could be a public

to ensure that the enterprise’s

cloud IaaS that is affected by an attack

contracted capacity is always available

exploiting vulnerabilities of software

and cannot be directed to other tenants

installed by one of the tenants.

without approval.

• Use a private cloud deployment model

(no multi-tenancy).

Hypervisor

Hypervisors are vital for server

• If possible include a right of audit in

attacks

virtualization. They provide the link
the contract.
between virtual machines and the
• Include in the contract language that
underlying physical resources required
requires the CSP to be aligned with the
to run the machines by using hypercalls
enterprise’s security policy and to
(similar to system calls, but for
implement necessary controls to
virtualized systems). An attacker using a
ensure it.
virtual machine in the same cloud could
fake hypercalls to inject malicious code
or trigger bugs in the hypervisor. This
could potentially be used to violate
confidentiality or integrity of other
virtual machines or crash the hypervisor
(similar to a DDoS attack).
Support for
Security audits and forensic

• Request the CSP the right to audit as
audit and
investigations are vital to the enterprise
part of the contract or SLA. If this is
forensic
to evaluate the security measures of the
not possible, request security audit
investigations
CSP (preventive and corrective), and in
reports by trusted third parties.
some cases the CSP itself (for example,
• Request that the CSP provide
to authenticate the CSP). This raises
appropriate and timely support (logs,
several issues because performing these
traces, hard disk images, etc.) for
actions requires extensive access to the
forensic analysis as part of the contract
CSP’s infrastructure and monitoring
or SLA. If this is not possible, request
capabilities, which are often shared with

to authorize trusted third parties to

other CSP’s customers.

perform forensic analysis when

necessary.

Source: Data from ISACA; *Security Considerations for Cloud Computing*, USA, 2012.

5.10 VIRTUALIZED ENVIRONMENTS

Virtualization provides an enterprise with a significant opportunity to increase efficiency and decrease costs in its IT operations. However, virtualization also introduces additional risk. At a high level, virtualization allows multiple OSs (guests) to coexist on the same physical server (host) in isolation of one another. Virtualization creates a layer between the hardware and the guest OSs to manage shared processing and memory resources on the host. Often, a management console provides administrative access to manage the virtualized system.

Data centers and many other organizations use virtualization techniques to create an abstraction of the physical hardware and make large pools of logical resources consisting of CPUs, memory, disks, file storage, applications and networking. This approach enables greater availability of these resources to the user base. The main focus of virtualization is to enable a single physical computing environment to run multiple logical, yet independent, systems at the same time.

The most common use for full virtualization is operational efficiency, which uses existing hardware more efficiently by placing greater loads on each computer. Second, using full virtualization of desktops enables end users to have one computer hosting multiple OSs if needed to support various OS-dependent applications. Furthermore, an IT organization can better control deployed OSs to ensure that they meet the organization’s security requirements, security threat and respective control requirements are dynamic, and the virtual desktop images can be changed to respond to new threats.

The virtualized computing environment is normally comprised of the following elements:

• Server or other hardware product

• Virtualization hypervisor: A piece of computer software, firmware or hardware that creates and runs virtual machine environment—normally called the “host.”

• Guest machine: Virtual environment elements (e.g., OS, switches, routers, firewalls, etc.) residing on the computer on which a hypervisor host machine has been installed

A fully virtualized environment can be deployed using one of the following methods:

• **Bare metal/native virtualization** occurs when the hypervisor runs directly on the underlying hardware, without a host OS.

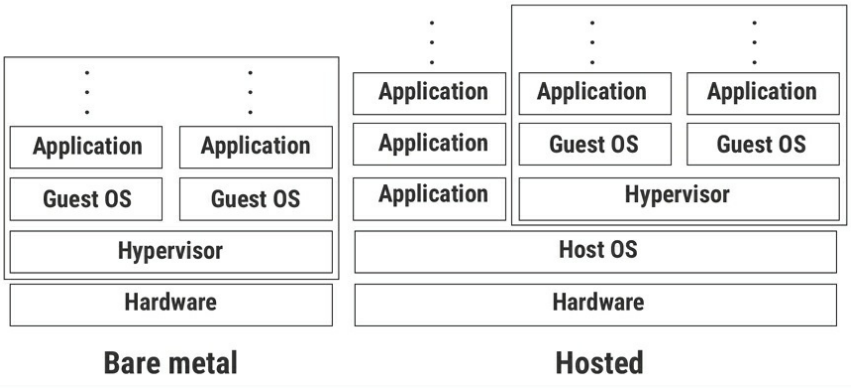
• **Hosted virtualization** occurs when the hypervisor runs on top of the host OS (Windows, Linux or MacOS). The hosted virtualization architectures usually have an additional layer of software (the virtualization application) running in the guest OS that provides utilities to control the virtualization while in the guest OS, such as the ability to share files with the host OS.

• **Containerization:** Containers include the application and all of its dependencies but share the kernel with other containers. They run as an isolated process in user space on the host operating system.

Figure 5.29 compares two of these architectures.

IS auditors need to understand the advantages and disadvantages of

Figure 5.29—Full Virtualization Architectures



virtualization to determine whether the enterprise has considered the applicable risk in its decision to adopt, implement and maintain this technology. **Figure 5.30** summarizes several advantages and disadvantages of virtualization.

Although virtualization offers significant advantages, they bring risk that an enterprise must manage effectively. Because the host in a virtualized environment represents a potential single point of failure within the system, a successful attack on the host could result in a compromise that is larger in both scope and impact.

Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

Figure 5.30—Advantages and Disadvantages of Virtualization

Advantages

Disadvantages

• Server hardware costs may decrease for both

• Inadequate configuration of the host could

server builds and server maintenance.

create vulnerabilities that affect not only the

• Multiple OSs can share processing capacity

host, but also the guests.

and storage space that often goes to waste in

• Exploits of vulnerabilities within the host’s

traditional servers, thereby reducing operating

configuration, or a denial of service attack

costs.

against the host, could affect all of the host’s

• The physical footprint of servers may decrease

guests.

within the data center.

• A compromise of the management console

• A single host can have multiple versions of the

could grant unapproved administrative access

same OS, or even different OSs, to facilitate

to the host’s guests.

testing of applications for performance

• Performance issues of the host’s own OS could

differences.

impact each of the host’s guests.

• Creation of duplicate copies of guests in

• Data could leak between guests if memory is

alternate locations can support business

not released and allocated by the host in a

continuity efforts.

controlled manner.

• Application support personnel can have

• Insecure protocols for remote access to the

multiple versions of the same OS, or even

management console and guests could result in

different OSs, on a single host to more easily

exposure of administrative credentials.

support users operating in different

environments.

• A single machine can house a multitier

network in an educational lab environment

without costly reconfigurations of physical

equipment.

• Smaller organizations that had performed tests

in the production environment may be better

able to set up logically separate, cost-effective

development and test environments.

• If set up correctly, a well-built, single access

control on the host can provide tighter control

for the host’s multiple guests.

To address risk, an enterprise can often implement and adapt the same principles and good practices for a virtualized server environment that it would use for a server farm. These include:

• Strong physical and logical access controls, especially over the host and its management console

• Sound configuration management practices and system hardening for the host, including patching, antivirus, limited services, logging, appropriate permissions and other configuration settings

• Appropriate network segregation, including the avoidance of virtual machines in the DMZ and the placement of management tools on a

separate network segment

• Strong change management practices

5.10.1 KEY RISK AREAS

Overall, migrating computing resources to a virtualized environment does not change the threat plane for most of the systems' vulnerabilities and threats. If a service has inherent vulnerabilities on a physical server or network product and it is migrated to a virtualized server, the service remains vulnerable to exploitation. However, the use of virtualization may also provide additional virtual environment attack vectors (e.g., hypervisor misconfiguration or security flaws, memory leakage, etc.), thus increasing the likelihood of successful attacks. The following types of high-level risk are representative of the majority of virtualized systems in use:

• Rootkits on the host installing themselves as a hypervisor below the OS, enabling the interception of any operations of the guest OS (i.e., logging password entry, etc.): Antivirus software may not detect this, because the malware runs below the entire OS.

• Default and/or improper configuration of the hypervisor partitioning resources (CPU, memory, disk space and storage): This can lead to unauthorized access to resources, one guest OS injecting malware into another or placing malware code into another guest OS's memory.

• On hosted virtualization, mechanisms called guest tools enable a guest OS

to access files, directories, the copy/paste buffer, and other resources on the host OS or another guest OS: This functionality can inadvertently provide an attack vector for malware or allow an attacker to gain access to particular resources. Snapshots/images of guests' environments contain sensitive data (such as passwords, personal data, etc.) like a physical hard drive: These snapshots pose a

greater risk than images because snapshots contain the contents of random access memory (RAM) at the time that the snapshot was taken, and this might include sensitive information that was not stored on the drive itself.

• In contrast to bare metal installations, hosted virtualization products rarely have hypervisor access controls: Therefore, anyone who can launch an application on the host OS can run the hypervisor. The only access control is whether someone can log into the host OS.

5.10.2 TYPICAL CONTROLS

An IS auditor should understand the following concepts:

• Hypervisors and guest images (OS and networks) are securely configured according to industry standards. Apply hardening to these virtual components as closely as one would to a physical server, switch, router, firewall or other computing device.

• Hypervisor management communications should be protected on a

dedicated management network. Management communications carried on untrusted networks should be encrypted, and encryption should encapsulate the management traffic.

• The hypervisor should be patched as the vendor releases the fixes.

• The virtualized infrastructure should be synchronized to a trusted

authoritative timeserver.

• Unused physical hardware should be disconnected from the host system.

• All hypervisor services, such as clipboard- or file-sharing between the guest OS and the host OS, should be disabled unless they are needed.

• Host inspection capabilities should be enabled to monitor the security of each guest OS. Hypervisor security services can allow security monitoring even when the guest OS is compromised.

• Host inspection capabilities should be enabled to monitor the security of

activity occurring between guest OSs. Of special focus is communications in a non-virtualized environment carried and monitored over networks by network security controls (such as network firewalls, security appliances, and network IDPS sensors).

• File integrity monitoring of the hypervisor should be used to monitor for signs of compromise.

5.11 MOBILE, WIRELESS AND INTERNET-OF-THINGS DEVICES

Portable and wireless devices present a ubiquitous threat to an enterprise's information assets and must be properly controlled. Policies and procedures and additional protection mechanisms must be put into place to ensure that data are protected to a greater extent on portable devices, because such devices will most likely operate in environments in which physical controls are lacking or nonexistent. Most mobile devices are easily lost or stolen and, thus, require the use of encryption technologies and strong authentication. It also may be necessary to classify some data as inappropriate for storage on a mobile device. The IS auditor should understand that all such media and devices can also be used by an individual to steal data and programs for personal use or gain.

5.11.1 MOBILE COMPUTING

Mobile computing refers to devices that are transported or moved during normal usage. Common mobile devices include tablets, smartphones, laptops, USB storage devices, digital cameras and other similar technologies. Their mobility makes it more difficult to implement logical and physical access

controls.

Figure 5.31 presents some known vulnerabilities and associated threats that need to be understood when dealing with mobile devices.

The following controls reduce the risk of disclosure of sensitive data stored on mobile devices. Many of these controls can be enforced by mobile device management (MDM) systems and/or secure containers (a separately

authenticated, encrypted area of the mobile device that is used to keep sensitive

enterprise data segregated from the personal data) for enterprise and personal devices:

• **Device registration**—All mobile devices authorized for business use should be registered in a database. Devices that are personally owned should be flagged. Organizations can push updates or manage authorized devices and exclude personally owned mobile devices.

• **Tagging**—Physically tagging the device with an asset ID may result in its return if it is lost; however, there is risk in identifying the organization that owns the device.

• **Physical security**—If the device is stationary and permits it, use a cable locking system or a locking system with a motion detector that sounds an audible alarm.

• **Data storage**—Only store content that is absolutely needed on the device.

With the ability to remotely access central servers, the requirement to store any data locally should be questioned. If data are not stored locally, then a lost or stolen device will not be an issue. The data that are stored should be backed up on a regular basis, preferably to shared folders on the enterprise's file server.

Figure 5.31—Mobile Device Vulnerabilities, Threats and Risk

Vulnerability

Threat

Risk

Information travels across

Malicious outsiders can do harm

Information interception

wireless networks that are

to the enterprise.

resulting in a breach of sensitive

often less secure than wired

data, enterprise reputation,

networks.

adherence to regulation or legal

action

Mobility provides users with

Mobile devices cross boundaries

Malware propagation, which may

the opportunity to leave

and network perimeters, carrying

result in data leakage, data

enterprise boundaries and

malware, and can bring this

corruption and unavailability of

thereby eliminates many

malware into the enterprise

necessary data

security controls.

network.

Bluetooth technology is

Hackers can discover the device

Device corruption, lost data, call

very convenient for many

and launch an attack.

interception, possible exposure of

users to have hands-free

sensitive information

conversations; however, it is

often left on and then is

discoverable.

Unencrypted information is

In the event that a malicious

Exposure of sensitive data,

stored on the device.

outsider intercepts data in transit

resulting in damage to the

or steals a device or if the

enterprise, customers or

employee loses the device, the

employees

data are readable and usable.

Lost data may affect

Mobile devices may be lost or

Workers dependent on mobile

employee productivity.

stolen due to their portability.

devices unable to work in the

Data on these devices are not

event of broken, lost or stolen

always backed up.

devices and data that are not

backed up

The device has no

In the event that the device is lost

Data exposure, resulting in

authentication requirements

or stolen, outsiders can access the

damage to the enterprise and

applied.

device and all of its data.

liability and regulation issues

The enterprise is not

If no mobile device strategy
Data leakage, malware
managing the device.
exists, employees may choose to
propagation or unknown data
bring in their own unsecured
loss in the case of device loss or
devices.
theft.
The device allows for
Applications may carry malware
Malware propagation, data
installation of unsigned
that propagates Trojans or
leakage or intrusion on enterprise
third-party applications.
viruses; the applications may also
network
transform the device into a
gateway for malicious outsiders
to enter the enterprise network.

Source: ISACA, *Securing Mobile Devices*, USA, 2012

• **Virus detection and control**—The threat associated with viruses applies to all mobile devices. The enterprise should update the mobile device antivirus software to prevent perpetuation of malware.

• **Encryption**—Mobile devices used to store sensitive or confidential information should be encrypted in accordance with the organization's information security policies, mandating use of a strong encryption mechanism.

• **Compliance**—Mobile devices should comply with the security requirements as defined in enterprise standards. All mobile devices should require a password. Two-factor authentication can be used to further enhance security.

• **Approval**—Mobile-device use should be appropriately authorized and approved in accordance with the organization's policies and procedures.

• **Acceptable use policy**—A security policy should exist for mobile devices.

The enterprise should have a policy that addresses mobile device use and specifies the type of information and kind of devices and information services that may be accessible through the devices.

• **Due care**—Employees should exercise due care within office environments and especially during travel. Any loss or theft of a mobile device must be treated as a security breach and reported immediately in accordance to security management policies and procedures.

• **Awareness training**—Employee orientation and security awareness training should include coverage of mobile device policy and guidelines.

The training will allow propagation of awareness that mobile devices are important business tools when used properly and have risk associated with them, if not managed accordingly.

• **Network authentication, authorization and accounting**—IT

organizations should adopt a solution that allows them to tie devices connecting to the network with each user's identity and role, and then apply role-based policies to grant proper access privileges. This enables IT

to differentiate access for different levels of employees, guests or device type. It also lets IT take a proactive stance on tracking and monitoring how mobile devices are being used within the network.

• **Secure transmission**—Mobile devices should connect to the enterprise network via a secure connection, such as over a VPN.

• **Standard mobile device applications**—Configuration and use of the mobile device should be baselined and controlled. Only applications that either meet with the enterprise security architecture or are delivered as standard on the mobile device should be authorized for use, and all software applications must be appropriately licensed and installed by the organization's IS support team. MDM solutions support this.

• **Geolocation tracking**—There are many debates about the privacy concerns of GPS tracking, but location capabilities inherent in mobile

devices can be invaluable in the case of loss or theft.

• **Remote wipe and lock**—Due to the nature of mobile devices, many device management solutions are focused on securing the device if it is lost or stolen. Some MDM solutions allow IT to send an alarm to the device to help identify the location for a user, and, if truly lost, IT can then remotely wipe and lock the device and/or container.

• **Secure remote support**—Employees relying on personal devices to conduct work are often out of the office. Having a secure way to support and fix these devices from a remote location is imperative to maintain employee satisfaction. Depending on device type, remote support solutions allow help desks to configure devices, chat, transfer files, and remotely see and control the device. It is important to select a solution that supports a wide variety of devices and keeps all access and activity logs behind the enterprise firewall to ensure security.

Bring Your Own Device

Bring your own device (BYOD) is a current trend where personal

communication devices are being used to conduct work-related tasks. BYOD

offers many benefits to organizations that choose to adopt the practice, including

the following:

• Increased productivity and employee satisfaction by allowing employees to use their own devices

• Cost savings due to reduction of investment to procure and maintain end-user hardware and software licenses

• Employee satisfaction leading to higher productivity and innovation Security and control issues related to BYOD include the following:

• Protection of sensitive data and intellectual property

• Protection of networks to which BYOD devices connect

• Responsibility and accountability for the device and information contained on it

• Removal of the organization’s data from employee-owned devices on termination of employment or loss of the device

• Malware protection

Risk related to BYOD is similar to mobile computing risk. Some specific

BYOD-related risk is:

• Access controls and control over device security

• Ability to eliminate sensitive enterprise data on termination of employment or loss of the device

• Management issues related to supporting many different types of devices, operating systems and applications

• Ensuring that employee-owned BYOD devices are properly backed up at all times

An employee BYOD agreement or acceptable use agreement (AUA) should require the employee to agree with the items in the policy before the device can be used for business purposes. It may also state that devices can be seized, if

necessary, for a legal matter. An AUA ensures that maintaining security when using personal devices is a responsibility that is shared between the user and IT. In addition, BYOD should be approved by executive management and be subject to oversight and monitoring.

Internet Access on Mobile Devices

Smartphones and other mobile devices access the Internet by connecting to WLANs. These devices can also connect to the Internet over mobile networks.

Most mobile devices use third generation (3G) or fourth generation (4G) networks to connect to the Internet. 3G brought advances in Internet access times and download speeds. 4G is IP packet-switched network that adds VoIP, mobile TV and further speed increases. These developments have also led to changes in the way Internet content is accessed, with applications that are supported and access through an Internet browser.

The following are general issues and exposures that are related to wireless and/or mobile access:

• **The interception of sensitive information**—Information is transmitted through the air, which increases the potential for unprotected information to be intercepted by unauthorized individuals.

• **The loss or theft of devices**—Devices tend to be relatively small, making them much easier to steal or lose.

• **The loss of data contained in the devices**—Theft or loss can result in the loss of data that has been stored on the device. This could be several gigabytes depending on the capacity of the device. If encryption is weak or not applied, a hacker may access the information because it may only be protected by a password or PIN.

• **The misuse of devices**—Devices can be used to gather information or intercept information that is being passed over wireless networks for financial or personal benefit.

• **Distractions caused by the devices**—The use of the devices may distract the user. If these devices are being used in situations where an individual's full attention is required (e.g., driving a car), they could result in an increase in the

number of accidents.

• **Possible health effects of device usage**—The safety or health hazards have not yet been identified. However, there are a number of concerns with respect to electromagnetic radiation, especially for those devices that must be held beside the head.

• **OS vulnerabilities**—The OS may contain vulnerabilities that allow access to the device. Vulnerabilities, for example, allow devices to be jail broken, which means that restrictions have been intentionally removed from a device, allowing some enhancements, but potentially making it more vulnerable.

• **Applications**—Apps may contain vulnerabilities or malicious code that can allow access to data and the device itself. Jailbroken devices may be more susceptible to this because the apps may not come from secure sources.

• **Wireless user authentication**—There is a need for stronger user authentication and authorization tools at the device level. The current technology is just emerging.

• **File security**—Wireless phones and tablets do not use the type of file access security that other computer platforms can provide.

• **Wired equivalent privacy (WEP) security encryption**—WEP security depends particularly on the length of the encryption key and on the usage of static WEP (many users on a WLAN share the same key) or dynamic WEP (per-user, per-session, dynamic WEP key tied to the network logon).

The 64-bit encryption keys that are in use in the WEP standard encryption can be easily broken by the currently available computing power. Static

WEP, used in many WLANs for flexibility purposes, is a serious security risk, because a static key can easily be lost or broken, and if this has occurs, all of the information is available for viewing and use. An attacker possessing the WEP key can also sniff packets being transmitted and decrypt them. WEP is rarely used today because it has been deprecated.

WPA2 is the preferred solution for wireless networks.

5.11.2 WIRELESS NETWORKS

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections (i.e., without requiring network or peripheral cabling). Wireless is a technology that enables organizations to adopt ebusiness solutions with tremendous growth potential. Wireless technologies use radio frequency transmissions/electromagnetic signals through free space as the means for transmitting data, whereas wired technologies use electrical signals through cables. Wireless technologies range from complex systems (e.g., wireless wide area networks [WWANs], WLANs and cell phones) to simple devices (e.g., wireless headphones, microphones and other devices that do not process or store information).

Wireless technologies also include Bluetooth devices with a miniradio frequency transceiver and infrared devices, such as remote controls, cordless computer keyboards and mice and wireless headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link.

However, going wireless introduces new elements that must be addressed.

For example, existing applications may need to be retrofitted to make use of wireless interfaces. Also, decisions need to be made regarding general connectivity—to facilitate the development of completely wireless mobile applications or other applications that rely on synchronization of data transfer between mobile computing systems and enterprise infrastructure. Other issues include narrow bandwidth, the lack of a mature standard, and unresolved security and privacy issues.

Wireless networks serve as the transport mechanism between devices, and among devices and the traditional wired networks. Wireless networks are many and diverse but are frequently categorized into four groups based on their coverage range:

• WWANs

• WLANs

• Wireless personal area networks (WPANs)

• Wireless ad hoc networks

Wireless Wide Area Networks

Wireless wide area networking is the process of linking different networks over a large geographical area to allow wider IT resource sharing and connectivity. While computers are often connected to traditional WANs using cable networking solutions (such as telephone systems), wireless wide area networks are connected via radio, satellite and mobile phone technologies.

WWANs, using radio, satellite and mobile phone technologies, can complement and compete with more traditional systems of cable-based networking. These include wide coverage area technologies, such as Long-term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX), Cellular Digital Packet Data (CDPD), global system for mobile communications (GSM) and Mobitex.

For some organizations, such as those in rural areas where laying cable is too expensive, wireless technology offers the only networking solution. For others, wireless wide area networking provides greater system flexibility, and the opportunity to control costs where the equipment is owned.

Implementing a WWAN requires careful attention to the planning and surveying of the network. The total cost of ownership involved in switching to this rapidly evolving system of networking should also be considered.

Wireless Local Area Networks

WLANs allow greater flexibility and portability than traditional wired LANs.

Unlike a traditional LAN, which requires a wire to connect a user’s computer to the network, a WLAN connects computers, tablets, smartphones and other components to the network using an access point device. An access point, or wireless networking hub, communicates with devices equipped with wireless network adaptors within a specific range of the access point; it connects to a

wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (approximately 100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network devices. Access point cells can be linked together to allow users to roam within a building or between buildings. WLAN includes 802.11, HyperLAN, HomeRF and several others. WLANs are commonly

referred to as Wi-Fi hotspots.

WLAN technologies conform to a variety of standards and offer varying levels of security features. The principal advantages of standards are to encourage mass production and to allow products from multiple vendors to interoperate. The most useful standard used currently is the IEEE 802.11

standard.

802.11 refers to a family of specifications for WLAN technology. 802.11

specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

Note: The CISA candidate will not be tested on these IEEE standards in the exam.

WEP and Wi-fi Protected Access (WPA/WPA2)

IEEE 802.11's WEP encryption uses symmetric, private keys, which means the end user's radio-based NIC and access point must have the same key.

Symmetric, private keys cause difficulties periodically when distributing new keys to each NIC. As a result, keys remain unchanged on networks for extended times. With static keys, several hacking tools can easily break through the relatively weak WEP encryption mechanisms.

Because of the key-reuse problem and other flaws, the current standardized version of WEP does not offer strong enough security for most enterprise applications. Newer security protocols, such as 802.11i (WPA2) and Wi-Fi Protected Access (WPA), however, use public key cryptography techniques to provide effective authentication and encryption between users and access points.

Wireless Personal Area Networks

WPANs are short-range wireless networks that connect wireless devices to one another. The most dominant form of WPAN technology is Bluetooth, which links wireless devices at very short distances. The oldest way to connect devices in a WPAN fashion is IR communications.

Bluetooth is an open-source standard that borrows many features from existing wireless standards, such as IEEE 802.11, IrDA, Digital Enhanced Cordless

Telecommunications (DECT), Motorola's Piano and TCP/IP, to connect portable devices without wires, via short-range radio frequencies (RF).

Bluetooth is a wireless protocol that connects devices within a range of up to 49 feet (15 meters) and has become a feature on some tablets, mobile phones, PC keyboards, mice, printers, etc. It is a system that changes frequencies from moment to moment using a technique called frequency-hopping.

Bluetooth is used in computer systems, especially laptops, as a replacement for physical cables and for infrared connections, which are limited to line of sight. Bluetooth devices find one another when they are in range and automatically set up a background connection.

Bluetooth allows for high data speeds (between 1 Mbps and 2 Mbps) but is designed only for peer-to-peer data transfer. An alternative form of WPAN

technology, called ZigBee, offers slower data speeds (250 Kbps) than Bluetooth, but is both cheaper than Bluetooth and requires far less energy to power.

Ad Hoc Networks

Ad hoc networks are designed to dynamically connect remote devices, such as mobile phones, laptops and tablets. These networks are termed ad hoc because of their shifting network topologies. Whereas WLANs or WPANs use a fixed network infrastructure, ad hoc networks maintain random network configurations, relying on a system of mobile routers connected by wireless links to enable devices to communicate. Bluetooth networks can behave as ad hoc networks, because mobile routers control the changing network topologies of these networks.

The routers also control the flow of data between devices that are capable of supporting direct links to each other. As devices move about in an unpredictable fashion, these networks must be reconfigured to handle the dynamic topology. The routing protocol employed in Bluetooth allows the routers to establish and maintain these shifting networks.

The mobile router is commonly integrated in a handheld device. This mobile router, when configured, ensures that a remote, mobile device, such as a mobile phone, stays connected to the network. The router maintains the connection and controls the flow of communication.

Public Global Internet Infrastructure

The Internet is a vast, global network of networks, ranging from university networks to corporate LANs to large online services. The Internet is not run or controlled by any single person, group or organization. The only thing that is centrally controlled is the availability and assignment of Internet addresses and the attached symbolic host names. Addresses and names are used for locating the source or destination networks.

Users can access the Internet through wireless-enabled devices or an ISP.

Routers, which connect networks, perform most of the work of directing traffic on the Internet. Networks are connected in different ways including telephone lines, ISDN telephone lines, leased lines, fiber-optic cables and satellite.

The networks in a particular geographic area are connected into a large regional network. Regional networks are connected to one another via high-speed backbones (connections that can send data at extremely high speeds).

When data are sent from one regional network to another, they first travel to a network access point (NAP). NAPs then route the data to high-speed backbone network services (BNS). The data are then sent along the backbone to another regional network and then to a specific network and computer within that regional network.

Wireless Security Threats and Risk Mitigation

The classification of security threats can be segmented into the following

nine categories:

• Errors and omissions

• Fraud and theft committed by authorized or unauthorized users of the system

• Employee sabotage

• Loss of physical and infrastructure support

• Malicious hackers

• Industrial espionage

• Malicious code

• Foreign government espionage

• Threats to personal privacy

All of these represent potential threats in wired networks as well. However, the more immediate concerns for wireless communications are device theft, DoS, malicious hackers, malicious code, theft of service, and industrial and foreign government espionage.

Theft is likely to occur with wireless devices because of their portability.

Authorized and unauthorized users of the system may commit fraud and theft; however, authorized users are more likely to carry out such acts.

Because users of a system may know what resources a system has and the system's security flaws, it is easier for them to commit fraud and theft.

Malicious hackers, sometimes called crackers, are individuals who break into a system without authorization, usually for personal gain or to do harm. Such hackers may gain access to the wireless network access point by

eavesdropping on wireless device communications.

Malicious code involves viruses, worms, Trojan horses, logic bombs or other unwanted software that is intended to damage files or bring down a system.

Theft of service occurs when an unauthorized user gains access to the network and consumes network resources. In wireless networks, the unauthorized access threat stems from the relative ease with which eavesdropping can occur on radio transmissions.

Ensuring confidentiality, integrity and availability are the prime objectives in

wireless networks.

Security requirements include the following:

• **Authenticity**—A third party must be able to verify that the content of a message has not been changed in transit.

• **Nonrepudiation**—The origin or the receipt of a specific message must be verifiable by a third party.

• **Accountability**—The actions of an entity must be uniquely traceable to that entity.

• **Network availability**—The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses.

Availability also includes ensuring that resources are used only for intended purposes.

Risk in wireless networks is equal to the sum of the risk of operating a wired network plus the new risk introduced by weaknesses in wireless protocols. To mitigate the risk, an organization must adopt security measures and practices that help bring risk to a manageable level.

Following are some of the more salient threats and vulnerabilities of wireless systems:

• All of the vulnerabilities that exist in a conventional wired network apply to wireless technologies.

• Weaknesses in wireless protocols increase the threat of disclosure of sensitive information. Many wireless networks are either not secure or use outdated encryption algorithms.

• Malicious entities may gain unauthorized access to an agency’s computer or voice (IP telephony) network through wireless connections, potentially bypassing any firewall protections.

• Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and is transmitted between two wireless devices may be intercepted and disclosed.

• DoS attacks may be directed at wireless connections or devices.

• Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.

• Sensitive data may be corrupted during improper synchronization.

• Malicious entities may be able to violate the privacy of legitimate users and track their physical movements.

• Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.

• Mobile devices are easily stolen and can reveal sensitive information.

• Data may be extracted without detection from improperly configured devices.

• Viruses or other malicious code may corrupt data on a wireless device and be subsequently introduced to a wired network connection.

• Malicious entities may, through wireless connections, connect to other agencies for the purposes of launching attacks and concealing their activity.

• Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

• Malicious entities may use a third-party, untrusted wireless network service to gain access to the network resources.

Another problem with WPANs is the uncontrolled propagation of radio waves; for example, the radio traffic on Bluetooth connections can be passively intercepted and recorded using Bluetooth protocol sniffers, such as Red Fang, Bluesniff and others. If the device addresses are known, then even if the devices are currently in nondiscoverable mode, it is possible to synchronize to the frequency hopping sequence. All the layers of the Bluetooth protocol stack can be examined and analyzed offline. If encryption is not used, then it is possible to extract and monitor the transmitted user data.

Use of an antenna with a strong directional characteristic and electronics that are capable of amplifying Bluetooth signals can make passive listening attacks possible from a greater distance than the functional range.

Transmitting power control is optional and is not supported by every Bluetooth device.

5.11.3 INTERNET OF THINGS

Internet of Things (IoT) refers to physical objects that have embedded network and computing elements and communicate with other objects over a network. Definitions of IoT vary about the pathway of communication and whether the object communicates over an Internet connection or a network

connection without the Internet.

This growing internetwork of things is comprised of physical objects with the capability to communicate in new ways—with each other, with their owners or operators, with their manufacturers or with others—to make people's lives easier and enterprises more efficient and competitive.

Business value and organizational competitiveness can be derived as enterprises capitalize on IoT capabilities to gain more and better business value from devices that they purchase. Additionally, businesses can compete more effectively in the marketplace because they provide these features in products that they sell and incorporate them into service offerings that they provide.

However, with that additional value comes additional risk. Although specific risk depends on usage, some of the IoT-usage risk areas that practitioners should consider are:

• Business risk:

– Health and safety

– Regulatory compliance

– User privacy

– Unexpected costs

• Operational risk:

– Inappropriate access to functionality

– Shadow usage

– Performance

• Technical risk:

– Device vulnerabilities

– Device updates

– Device management

PART B: SECURITY EVENT MANAGEMENT

Business environments are internetworked with public and private networks, providing additional opportunity for unauthorized access. Barriers, alarms and alerts, network layering, and system and perimeter security provide a level of security. However, internal and external security breaches continue to occur because of new threats and vulnerabilities. The response to these incidents is a critical component of business continuity, risk management, the maintenance and management of the security infrastructure and, in some cases, compliance with rules and regulations. The fundamental component of incident response/handling is to implement timely remediation action with minimal disruption of information services, until such time that a disruption can be accommodated with minimal impact to the enterprise.

5.12 SECURITY AWARENESS TRAINING AND PROGRAMS

Risk that is inherent in using computing systems cannot be addressed through technical security mechanisms. An active security awareness program can greatly reduce risk by addressing the behavioral element of security through education and consistent application of awareness techniques. Security awareness programs should focus on common user security concerns—such as password selection, appropriate use of computing resources, email and web browsing safety, and social engineering—and the programs should be tailored to specific groups. In addition, users are the front line for the detection of threats that may not be detectable by automated means (e.g., fraudulent activity and social engineering). Employees should be educated on recognizing and

escalating such events to enhance loss prevention.

An important aspect of ensuring compliance with the information security program is the education and awareness of the organization regarding the importance of the program. In addition to the need for information security,

all personnel must be trained in their specific responsibilities related to information security.

Particular attention must be paid to job functions that require virtually unlimited data access. People whose job is to transfer data may have access to data in most systems, and those doing performance tuning can change most OS configurations. People whose job is to schedule batch jobs have the authority to run most system jobs applications. Programmers have access to change application code. These functions are not typically managed by information security. Although it is possible to set up elaborate monitoring controls, it is not technically feasible or financially prudent for information security to provide oversight adequate to ensure that all data transfer jobs that transmit reports send them only to appropriately authorized recipients.

Although information security can ensure that there is clear policy, develop applicable standards and assist in process coordination, management in all areas must assist in providing oversight.

Employee awareness should start from the point of joining the organization (e.g., through induction training) and continue regularly. Techniques for delivery need to vary to prevent them from becoming stale or boring and may also need to be incorporated into other organizational training programs.

Security awareness programs should consist of:

• Training

• Quizzes to gauge retention of training concepts

• Security awareness reminders, such as posters, newsletters or screensavers

• A regular schedule of refresher training

In larger organizations, there may be a large enough population of middle and

senior management to warrant special management-level training on information security awareness and operations issues.

All employees of an organization and, where relevant, third-party users must receive appropriate training and regular updates on the importance of security policies, standards and procedures in the organization. This includes security requirements, legal responsibilities and business controls, as well as training

in the correct use of information processing facilities (e.g., login procedures, use of software packages). For new employees, this should occur before access to information or services is granted and be a part of new employee orientation.

A methodical approach should be taken to developing and implementing the education and awareness program with the following aspects being considered:

• Who is the intended audience (senior management, business managers, IT

staff, end users)?

• What is the intended message (policies, procedures, recent events)?

• What is the intended result (improved policy compliance, behavioral change, better practices)?

• What communication method will be used (computer-based training

[CBT], all-hands meeting, intranet, newsletters, etc.)?

• What is the organizational structure and culture?

Mechanisms for raising information security awareness include the following:

• Computer-based security awareness and training programs

• Email reminders and security tips

• Written security policies and procedures (and updates)

• Nondisclosure statements signed by the employee

• Use of different media in promulgating security (e.g., company newsletter, web

page, videos, posters, login reminders)

• Visible enforcement of security rules

• Simulated security incidents for improving security

• Rewarding employees who report suspicious events

• Periodic reviews

• Job descriptions

• Performance reviews

A second critical success factor to information security management is that a professional risk-based approach must be used systematically to identify sensitive and critical information resources and to ensure that there is a clear understanding of threats and risk. Thereafter, appropriate risk assessment

activities should be undertaken to mitigate unacceptable risk and ensure that residual risk is at an acceptable level.

5.13 INFORMATION SYSTEM ATTACK METHODS AND TECHNIQUES

Risk arises from vulnerabilities (whether technical or human) within an environment. Attack techniques exploit those vulnerabilities and may originate either within or outside the enterprise. Computer attacks can result in proprietary or confidential data being stolen or modified, loss of customer confidence and market share, embarrassment to management, and legal actions against an enterprise. Understanding the methods, techniques and exploits that are used to compromise an environment provides the IS auditor with a more complete context for understanding the risk that an enterprise faces.

Taking these techniques into consideration and understanding that they can be launched from any location allow for more thorough evaluations, ultimately providing a more secure environment. The IS auditor should understand enough of these attack types to recognize their risk to the business and how they should be addressed by appropriate controls.

5.13.1 FRAUD RISK FACTORS

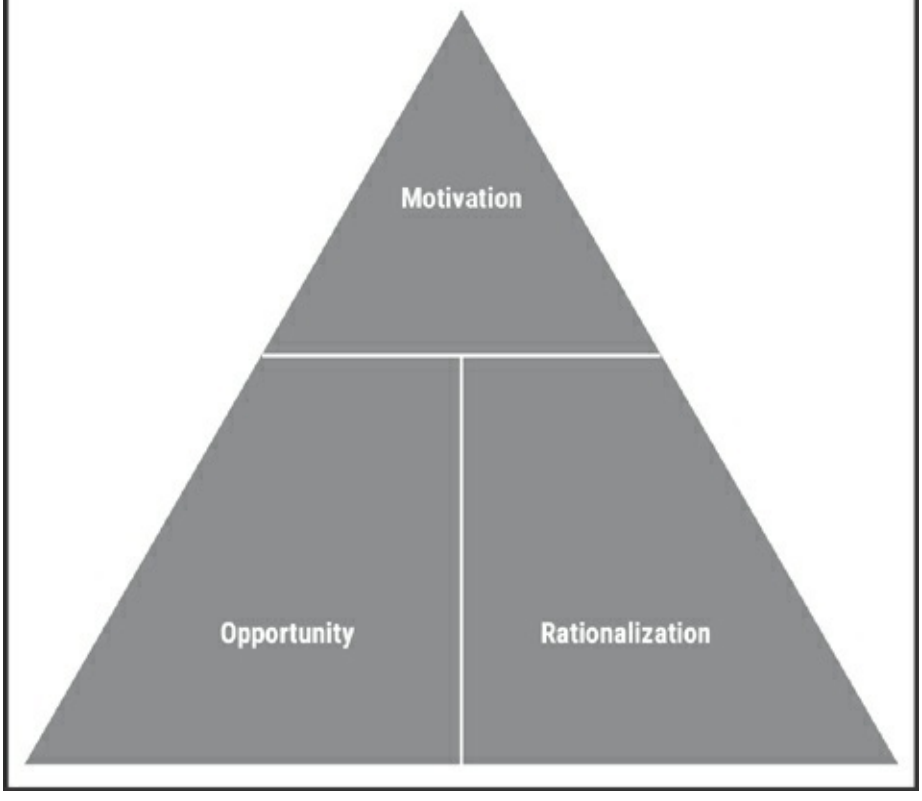
Fraud is the crime of using dishonest methods to take something valuable from a person or organization. There can be many reasons why a person commits fraud, but one of the more accepted models is the fraud triangle

(figure 5.32), which was developed by criminologist Donald R. Cressey in the 1950s. Cressey believed that the three key elements in the fraud triangle are opportunity, motivation and rationalization:

• **Motivation** refers to a perceived financial (or other) need. The fraudster may be in debt, hold a personal grudge, have a problem with drugs or gambling, or want to enjoy status symbols, such as a bigger house or car.

• **Rationalization** refers to the way the fraudster justifies the crime to themselves. Rationalization may include thoughts such as, “I deserved the money,” “I was only borrowing the money,” “my family needs the

Figure 5.32—The Fraud Triangle



money,” “my employer has loads of money anyway,” or “my employer treats me

unfairly.”

• **Opportunity** refers to the method by which the crime is to be committed.

Opportunity is created by abuse of position and authority, poor internal controls, poor management oversight, etc. Failure to establish procedures to detect fraud increases the likelihood of fraud occurring. Opportunity is the element over which organizations—and, by extension, IS auditors—

have the most control. When considering information assets, the

opportunities to commit fraud can be limited by security controls. These controls typically include logical access (including those for third parties), segregation of duties (SoD), human resources security, etc.

Source: Association of Certified Fraud Examiners, “The Fraud Triangle,” *http://www.acfe.com/fraud-*

triangle.aspx

5.13.2 COMPUTER CRIME ISSUES AND EXPOSURES

Computer systems can be used to fraudulently obtain money, goods, software

or enterprise information. Crimes can also be committed when the computer application process or data are manipulated to accept false or unauthorized transactions. There is also the simple, nontechnical method of computer crime: stealing computer equipment.

Computer crime can be performed without anything physically being taken or stolen, and it can be done remotely. Simply viewing computerized data can provide an offender with enough intelligence to steal ideas or confidential information (intellectual property). In case of the systems connected to WANs or the Internet, the crime scene could be anywhere in the world, making the investigation very difficult. Cybercriminals take advantage of existing gaps in the legislation of different countries when planning cyberattacks in order to avoid prosecution.

Committing crimes that exploit the computer and the information it contains can be damaging to the reputation, morale and the continued existence of an

organization. Loss of customers or market share, embarrassment to management and legal actions against the organization can result. Threats to business include:

• **Financial loss**—These losses can be direct, through loss of electronic funds, or indirect, through the costs of correcting the exposure.

• **Legal repercussions**—There are numerous privacy and human rights laws an organization should consider when developing security policies and procedures. These laws can protect the organization but also can protect the perpetrator from prosecution. In addition, not having proper security measures could expose the organization to lawsuits from investors and insurers if a significant loss occurs from a security violation. Most companies must also comply with industry-specific regulatory agencies'

requirements. The IS auditor should obtain legal assistance when reviewing the legal issues associated with computer security.

• **Loss of credibility or competitive edge**—Many organizations, especially service firms, such as banks, savings and loans and investment firms, need credibility and public trust to maintain a competitive edge. A security violation can damage this credibility severely, resulting in loss of business and prestige.

• **Blackmail/industrial espionage/organized crime**—By gaining access to

confidential information or the means to adversely impact computer operations, a perpetrator can extort payments or services from an organization by threatening to exploit the security breach or publicly disclose the confidential information of the organization. Also, by gaining access, the perpetrator could obtain proprietary information and sell it to a competitor.

• **Disclosure of confidential, sensitive or embarrassing information**—As noted previously, such events can damage an organization's credibility and its means of conducting business. Legal or regulatory actions against the company may also be the result of disclosure.

• **Sabotage**—Some perpetrators are not looking for financial gain. They merely want to cause damage due to a dislike of the organization or for self-gratification. Hacktivism occurs when perpetrators make nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends.

It is important that the IS auditor knows and understands the differences between computer crime and computer abuse to support risk analysis methodologies and related control practices. What constitutes a crime depends on the jurisdiction and the court sentence. Certain breaches of security may be civil or criminal offenses. This brings into play requirements for what the organization needs to do should a crime be suspected (i.e., protection of evidence, reporting of a crime, etc.).

Perpetrators in computer crimes are often the same people who exploit physical exposures, although the skills needed to exploit logical exposures are more technical and complex. Possible perpetrators include:

• **Hackers (also referred to as crackers)**—Persons with the ability to explore the details of programmable systems and the knowledge to stretch or exploit their capabilities, whether ethical or not. Hackers are typically attempting to test the limits of access restrictions to prove their ability to overcome the obstacles. Some often do not access a computer with the intent of destruction, although this is often the result. Types of hackers include hacktivists and criminal hackers. Some hackers seek to commit a crime through their actions for some level of personal gain or satisfaction.

The terms hack and crack are often used interchangeably.

• **Script kiddies**—Script kiddies refer to individuals who use scripts and

programs written by others to perform their intrusions and are often incapable of writing similar scripts on their own.

• **Employees (authorized or unauthorized)**—Affiliated with the organization and given system access based on job responsibilities, these individuals can cause significant harm to an organization. Therefore, screening prospective employees through appropriate background checks is an important means of preventing computer crimes within the organization.

• **IT personnel**—These individuals have the easiest access to computerized information, as they are the custodians of this information. In addition to logical access controls, good SoD and supervision help in reducing logical access violations by these individuals.

• **End users**—Personnel who often have broad knowledge of the information

within the organization and have easy access to internal resources

• **Former employees**—Former employees who have left on unfavorable terms may have access if it was not immediately removed at the time of the employee's termination or if the system has back doors.

• **Nations**—As more critical infrastructure is controlled from the Internet (e.g., supervisory control and data acquisition [SCADA] systems) and more nation's key organizations and businesses rely on the Internet, it is not uncommon for nations to attack each other.

• **Interested or educated outsiders**—These may include:

– Competitors

– Terrorists

– Organized criminals

– Hackers looking for a challenge

– Script kiddies for the purpose of curiosity, joyriding and testing their newly acquired tools/scripts and exploits

– Crackers

– Phreakers

• **Part-time and temporary personnel**—Facility contractors, such as office cleaners often have a great deal of physical access and could perpetrate a computer crime.

• **Third parties**—Vendors, visitors, consultants or other third parties who, through projects, gain access to the organization's resources and could perpetrate a crime

• **Opportunists**—Where information is inadvertently left unattended or left

for destruction, a passerby can access same

• **Accidental unaware**—Someone who unknowingly perpetrates a violation

Other examples of criminals include hacktivists, small-time crooks, organized crime and state-sponsored criminal activities.

Although collaboration has been improved in solving cybercrimes committed from one country to another, political issues existing between some countries might hinder an investigation. Therefore, additional preventive measures should be taken to protect information systems vulnerable to international attacks.

Figures 5.33 and **5.34** describe common attack methods and techniques for computer crimes. Perpetrators may use one or more methods in tandem to commit a crime.

Figure 5.33—Computer Crimes

Source of the Attack	Target of the Attack	Examples
Computer is the target of the	Specific identified computer	• Denial of service (DoS)
crime.		• Hacking
Perpetrator uses another	computer to launch an attack.	
Computer is the subject of the	Target may or may not be	• Distributed DoS
crime.		

defined. Perpetrator launches the

• Malware

attack with no specific target in

Perpetrator uses computer to

mind.

commit crime and the target is

another computer.

Computer is the tool of the crime.

Target is data or information

• Fraud

stored on the computer.

• Unauthorized access

Perpetrator uses computer to

• Phishing

commit crime but the target is not

• Installing key loggers

the computer.

Computer symbolizes the crime.

Target is user of the computers.

• Social engineering

methods:

Perpetrator lures the user of

– Phishing

computers to get confidential

– Fake web sites

information.

– Scam mail

– Spam mail

– Fake resumes for

employment

Figure 5.34—Common Attack Methods and Techniques

Alteration Attack

Occurs when unauthorized modifications affect the integrity of the data or code

Examples: Unauthorized alteration of binary code during the software development life cycle (SDLC) or addition of unauthorized libraries during recompilation of existing programs

Cryptographic hash is a primary defense against alteration attacks.

Botnets

Comprise a collection of compromised computers (called zombie

computers) running software, usually installed via worms, Trojan horses or back doors

Examples: DoS attacks, adware, spyware and spam

Denial-of-service

Examples:

(DoS) Attack

ICMP flood attack:

• Smurf attack—Occurs when misconfigured network devices allow

packets to be sent to all hosts on a particular network via the broadcast address of the network

• Ping flood—Occurs when the target system is overwhelmed with ping packets

• SYN flood—Sends a flood of TCP/SYN packets with forged sender

address, causing half-open connections and saturates available

connection capacity of the target machine

Teardrop attack—Involves sending mangled IP fragments with

overlapping, oversized payloads to the target machine

Peer-to-peer attack—Causes clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's website instead. As a result, several thousand computers may aggressively try to connect to a target website, causing performance degradation.

Permanent denial-of-service (PDoS) attack (also known as phlashing)—

Damages a system hardware to the extent of replacement

Application-level flood attack:

• Buffer overflow consumes available memory or CPU time.

• Brute force attack—Floods the target with an overwhelming flux of packets, oversaturating its connection bandwidth or depleting the target's system resources

• Bandwidth-saturating flood attack—Relies on the attacker having higher

bandwidth available than the victim

• Banana attack—Redirects outgoing messages from the client back onto the client, preventing outside access, as well as flooding the client with

the sent packets

• Pulsing zombie—A DoS attack in which a network is subjected to hostile pinging by different attacker computers over an extended time period. This results in a degraded quality of service and increased workload for the network's resources.

Nuke—A DoS attack against computer networks in which fragmented or invalid ICMP packets are sent to the target. Modified ping utility is used to repeatedly send corrupt data, thus slowing down the affected computer to a complete stop.

Distributed denial-of-service attack (DDoS)—Occurs when multiple compromised systems flood the bandwidth or resources of the targeted system

Reflected attack—Involves sending forged requests to a large number of computers that will reply to the requests. The source IP address is spoofed to that of the targeted victim, causing the replies to flood.

Unintentional attack—Website ends up denied, not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity

Dial-in Penetration

An intruder determines the dial-in phone number ranges from external
Attack/War Dialing

sources, such as the Internet. The intruder may also employ social engineering tactics to get information from a company receptionist or a knowledgeable employee inside the company

Eavesdropping

An intruder gathers the information flowing through the network with the intent of acquiring and releasing the message contents for either personal analysis or

for third parties who might have commissioned such

eavesdropping. This is significant when considering that sensitive information, traversing a network, can be seen in real time by all other machines, including email, passwords and, in some cases, keystrokes.

These activities can enable the intruder to gain unauthorized access, to fraudulently use information, such as credit card accounts and to compromise the confidentiality of sensitive information that could jeopardize or harm an individual's or an organization's reputation.

Email Attacks and

Email Bombing—Characterized by abusers repeatedly sending an identical Techniques

email message to a particular address

Email spamming (also known as unsolicited commercial email (UCE) or junk email)—a variant of bombing and refers to sending email to hundreds or thousands of users (or to lists that expand to that many users). It may also occur innocently as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users or as a result of using a responder message, such as a vacation alert, that is not set up correctly.

• Spam causes inconvenience and has severe impacts on productivity and thus is considered a business risk.

• When spam is responded to, the email address of the recipient is validated and gives away information.

• Spam may be combined with email spoofing (see below), making it more difficult to determine from whom the email is coming.

• Spam is managed using the Sender Permitted Form (SPF) protocol and with the help of tools, such as Bayesian filtering and greylisting.

Email Spoofing—May occur in different forms, but all have a similar result: a user receives an email message that appears to have originated from one source but actually was sent from another source. Email spoofing is often an attempt to

trick the user into making a damaging statement or releasing sensitive information, such as passwords or account information.

Examples of spoofed email that could affect the security of a site include:

• Email claiming to be from a system administrator and requesting users to change their passwords to a specified string and threatening to suspend their account if they do not make the change

• Email claiming to be from a person in authority and requesting users to send a copy of a password file or other sensitive information

Phishing—The criminally fraudulent process of attempting to acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing techniques include social engineering, link manipulation and website forgery.

Spear phishing—A pinpoint attack against a subset of people (users of a website or product, employees of a company, members of an organization) to undermine that company or organization

Flooding

A DoS attack that brings down a network or service by flooding it with large amounts of traffic. The host's memory buffer is filled by flooding it with connections that cannot be completed.

Interrupt Attack

Occurs when a malicious action is performed by invoking the OS to execute a particular system call

Example: A boot sector virus typically issues an interrupt to execute a write to the boot sector.

Juice Jacking

Occurs when malware is surreptitiously installed on, or data are copied from, a smart phone, tablet or other device using an often public USB

charging port that doubles as a data connection

Malicious Codes

Trojan horses (often called Trojans)—Programs that are disguised as useful programs, such as OS patches, software packages or games. Once executed, however, Trojans perform actions that the user did not intend, such as opening certain ports for subsequent access by the intruder.

Logic bomb—A program or a section of a program that is triggered when a certain condition, time or event occurs. Logic bombs typically result in sabotage of computer systems and are commonly deployed by disgruntled insiders who have access to programs. For example, when terminated from

an organization, a disgruntled software programmer could devise a logical bomb to delete critical files or databases. Logic bombs can also be used against attackers. Administrators sometimes intentionally install pseudo flaws, also called honey tokens, that look vulnerable to attack but really act as alarms or triggers of automatic actions when the intruder attempts to exploit the flaw.

Trap doors—Commonly called back doors. Bits of code embedded in

programs by programmers to quickly gain access during the testing or debugging phase. If an unscrupulous programmer purposely leaves in this code (or simply forgets to remove it), a potential security hole is introduced. Hackers often plant a back door on previously compromised systems to gain subsequent access. Threat vector analysis (a type of defense-in-depth architecture), SoD and code audits help to defend against logic bombs and trap/back doors.

Man-in-the-middle

The following scenarios are possible:

Attack

• The attacker actively establishes a connection to two devices. The attacker connects to both devices and pretends to each of them to be the other device. Should the attacker’s device be required to authenticate itself to one of the devices, it passes the authentication request to the other device and then sends the response back to the first device. Having authenticated himself/herself in this

way, the attacker can then interact with the device as he/she wishes. To successfully execute this attack, both devices have to be connectable.

• The attacker interferes while the devices are establishing a connection.

During this process, the devices have to synchronize the hop sequence that is to be used. The aggressor can prevent this synchronization so that both devices use the same sequence but a different offset within the sequence.

Masquerading

An active attack in which the intruder presents an identity other than the original identity. The purpose is to gain access to sensitive data or computing/network resources to which access is not allowed under the original identity. Masquerading also attacks the authentication attribute by letting a genuine session authentication take place and subsequently enters the information flow, masquerading as one of the authenticated users of the session.

Impersonation both by people and machines falls under this category.

Masquerading by machines (also known as IP spoofing)—A forged IP

address is presented. This form of attack is often used as a means of breaking a firewall.

Message Modification

Involves the capturing of a message and making unauthorized changes or deletions (of full streams or parts of the message), changing the sequence or delaying transmission of captured messages. This attack can have disastrous effects if, for example, the message is an instruction to a bank to make a payment.

Network Analysis

An intruder applies a systematic and methodical approach known as footprinting to create a complete profile of an organization’s network security infrastructure. During this initial reconnaissance phase, the intruder uses a combination of tools and techniques to build a repository of information about a particular company’s internal network. This probably would include information about system aliases,

functions, internal addresses, and potential gateways and firewalls. Next, the intruder focuses on systems within the targeted address space that responded to these network queries. Once a system has been targeted, the intruder scans the system's ports to determine what services and OS are running on the targeted system, possibly revealing vulnerable services that could be exploited.

Packet Replay

A combination of passive and active modes of attacks. The intruder passively captures a stream of data packets as the stream moves along an unprotected or vulnerable network. These packets are then actively inserted into the network as if the stream were another genuine message stream. This form of attack is effective particularly where the receiving end of the communication channel is automated and will act on receipt and interpretation of information packets without human intervention.

Pharming

An attack that aims to redirect the traffic of a website to a bogus website.

Pharming can be conducted either by changing the host's file on a victim's computer or by exploiting a vulnerability in DNS server software. DNS

servers are computers responsible for resolving Internet names into their real addresses—they are the signposts of the Internet. Compromised DNS

servers are sometimes referred to as poisoned. In recent years, both pharming and phishing have been used to steal identity information.

Pharming has become a major concern to businesses hosting ecommerce and to online banking websites. Sophisticated measures known as

antipharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming.

Piggybacking

The act of following an authorized person through a secured door or electronically attaching to an authorized telecommunications link to intercept and possibly alter transmissions. Piggybacking is considered a physical access

exposure.

Race Conditions (Time

Exploit a small window of time between the time that the security control of Check [TOC]/Time

is applied and the time that the service is used. The exposure to a race of Use [TOU] attacks)

condition increases in proportion to the time difference between TOC and TOU. Interference occurs when a device or system attempts to perform two or more operations at the same time, but the nature of the device or system requires the operations to happen in proper sequence.

Race conditions occur due to interferences caused by the following conditions:

• Sequence or nonatomic—These conditions are caused by untrusted processes, such as those invoked by an attacker, that may get in between the steps of the secure program.

• Deadlock, livelock or locking failure—These conditions are caused by

trusted processes running the same program. Since these different processes may have the same privileges, they may interfere with each other, if not properly controlled.

Careful programming and good administration practices help to reduce race conditions.

Remote Maintenance

If not securely configured and controlled, can be used as an attack method Tools

by malicious hackers to remotely gain elevated access and cause damage to the target system

Resource Enumeration

When the attacker lists the various resources (names, directories, and Browsing

privileges, shares, policies) on targeted hosts and networks

Browsing attack—A form of a resource enumeration attack and is

performed by a manual search, frequently aided with commands and tools available in software, OSs or add-on utilities

Salami

Involves slicing small amounts of money from a computerized transaction or account. Similar to the rounding down technique. The difference between the rounding down technique and the salami technique is that, in rounding down, the program rounds off by the smallest money fraction.

For example, in the rounding down technique, a US $1,235,954.39

transaction may be rounded to US $1,235,954.35. On the other hand, the salami technique truncates the last few digits from the transaction amount, so US $1,235,954.39 becomes US $1,235,954.30 or $1,235,954.00,

depending on the algorithm/formula built into the program. In fact, other variations of the same technique are applied to rates and percentages.

Social Engineering

The human side of breaking into a computer system. Organizations with strong technical security countermeasures (such as authentication processes, firewalls and encryption) may still fail to protect their information systems. This situation may happen if an employee

unknowingly gives away confidential information (e.g., passwords and IP

addresses) by answering questions over the phone with someone they do not know or replying to an email message from an unknown person. Some examples of social engineering include impersonation through a telephone call, dumpster diving and shoulder surfing. The best means of defense for social engineering is an ongoing security awareness program, wherein all employees and third parties (who have access to the organization’s facilities) are educated about the risk involved in falling prey to social engineering attacks.

Traffic Analysis

An inference attack technique that studies the communication patterns between entities in a system and deduces information. This typically is used when messages are encrypted and eavesdropping would not yield meaningful results. Traffic analysis can be performed in the context of military intelligence or counter-intelligence and is a concern in computer security.

Unauthorized Access

Many Internet software packages contain vulnerabilities that render

Through the Internet or

systems subject to attack. Additionally, many of these systems are large Web-based Services

and difficult to configure, resulting in a large percentage of unauthorized access incidents.

Examples include:

• Email forgery (simple mail transfer protocol)

• Telnet passwords transmitted in the clear (via path between client and server)

• Altering the binding between IP addresses and domain names to

impersonate any type of server. As long as the DNS is vulnerable and used to map universal resource locators (URLs) to sites, there can be no integrity on the Web.

• Releasing common gateway interface (CGI) scripts as shareware. CGI scripts often run with privileges that give them complete control of a server.

• Client-side execution of scripts (via Java™ in Java applets), which presents the danger of running code from an arbitrary location on a client machine

Viruses, Worms and

Viruses—Involve the insertion of malicious program code into other

Spyware/Malware

executable code that can self-replicate and spread from computer to computer, via sharing of removable computer media, USB removable devices, transfer of logic over telecommunication lines or direct link with an infected machine/code. A virus can harmlessly display cute messages on computer terminals, dangerously erase or alter computer files, or simply fill computer memory with junk to a point where the computer can no longer function. An added danger is that a virus may lie dormant for some time until triggered by a certain event or occurrence, such as a date or being copied a prespecified number of times, during which time the virus has silently been spreading.

Worms—Destructive programs that may destroy data or use up

tremendous computer and communication resources, but worms do not replicate like viruses. Such programs do not change other programs but can run independently and travel from machine to machine across network connections by exploiting vulnerability and application/system

weaknesses. Worms also may have portions of themselves running on many different machines.

Spyware/Malware—Similar to viruses. Examples are keystroke loggers and system analyzers that collect potentially sensitive information, such as credit card numbers, bank details, etc., from the host and then transmit the information to the originator when an online connection is detected.

5.13.3 INTERNET THREATS AND SECURITY

The nature of the Internet makes it vulnerable to attack. The Internet is a global TCP/IP-based system that enables public and private heterogeneous networks to communicate with one another. Around 40 percent of the world's

population is connected to the Internet *(www.internetlivestats.com)*.

Originally designed to allow for the freest possible exchange of information, it is widely used today for commercial purposes. This poses significant security problems for organizations when protecting their information assets.

For example, hackers and virus writers try to attack the Internet and computers

connected to the Internet. Some want to invade others' privacy and attempt to crack into databases of sensitive information or sniff information as it travels across Internet routes. Consequently, it becomes more important for IS auditors to understand the risk and security factors that are needed to ensure that proper controls are in place when a company connects to the Internet.

The IP is designed solely for the addressing and routing of data packets across a network. It does not guarantee or provide evidence on the delivery of messages; there is no verification of an address; the sender will not know if the message reaches its destination at the time it is required; the receiver does not know if the message came from the address specified as the return address in the packet. Other protocols correct some of these drawbacks.

Network Security Threats

One class of network attacks involves probing for network information.

These passive attacks can lead to actual active attacks or

intrusions/penetrations into an organization's network. By probing for network information, the intruder obtains network information that can be used to target a particular system or set of systems during an actual attack.

Passive Attacks

Examples of passive attacks that gather network information include network analysis, eavesdropping and traffic analysis as explained in **figure 5.34**.

Active Attacks

Once enough network information has been gathered, the intruder will launch an actual attack against a targeted system to either gain complete control over that system or enough control to cause certain threats to be realized. This may include obtaining unauthorized access to modify data or programs, causing a DoS, escalating privileges, accessing other systems, and obtaining sensitive

information for personal gain. These types of penetrations or intrusions are known as active attacks. They affect the integrity, availability and authentication attributes of network security. Common forms of active attacks may include the following (explained in **figure 5.34**):

• Brute force attack

• Masquerading

• Packet replay

• Phishing

• Message modification

• Unauthorized access through the Internet

• Denial of service (DoS)

• Dial-in penetration attacks

• Email bombing and spamming

• Email spoofing

Causal Factors for Internet Attacks

Generally, Internet attacks of both a passive and active nature occur for a number of reasons including:

• Availability of tools and techniques on the Internet or as commercially available software that an intruder can download easily. For example, to scan ports, an intruder can easily obtain network scanners, such as strobe, netcat, jakal, nmap or Asmodeous (Windows). Additionally, password cracking programs, such as John the Ripper and L0phtCrack are available free or at a minimal cost.

• Lack of security awareness and training among an organization’s employees

• Exploitation of known security vulnerabilities in network-and host-based systems. Many organizations fail to properly configure their systems and to apply security patches or fixes when vulnerabilities are discovered. Most problems can be reduced significantly by keeping network- and host-based systems properly configured and up to date.

• Inadequate security over firewalls and host-based OSs allowing intruders to

view internal addresses and use network services indiscriminately With careful consideration when designing and developing network security controls and supporting processes, an organization can effectively prevent

and detect most intrusive attacks on its networks. In this situation, it becomes important for IS auditors to understand the risk and security factors that are needed to ensure proper controls are in place when a company connects to the Internet. There are several areas of control risk that must be evaluated by the IS auditor to determine the adequacy of Internet security controls.

5.13.4 MALWARE

The term malware is generally applied to a variety of malicious computer programs that send out requests to the OS of the host system under attack to append the malware to other programs. In this way, malware is self-propagating to other programs. They can be relatively benign (e.g., web application defacement) or malicious (e.g., deleting files, corrupting programs or causing a DoS). Generally, malware attack four parts of the computer:

• Executable program files

• The file-directory system, which tracks the location of all the computer's files

• Boot and system areas, which are needed to start the computer

• Data files

Another variant of malware frequently encountered is a worm, which, unlike a virus, does not physically attach itself to another program. To propagate itself to the host systems, a worm typically exploits security weaknesses in OSs' configurations. These problems are particularly severe in today's highly decentralized client-server environments. Currently, viruses or worms are transmitted easily from the Internet by downloading files to computers' web browsers. Malware are also transmitted as attachments to email, so that when the attachment opens, the system becomes infected if it is not using scanning software to review unopened attachments. Other methods of infection occur from files received through online services, social media, LANs and even shrink-wrapped software that the user may buy from a retail store.

Virus and Worm Controls

To effectively reduce the risk of computer viruses and worms infiltrating an organization, a comprehensive and dynamic anti-malware program needs to be established. There are two major ways to prevent and detect malware that

infect computers and network systems. The first is by having sound policies and procedures in place (preventive controls) and the second is by technical means (detective controls), including anti-malware software. Neither is effective without the other.

Management Procedural Controls

Some of the policy and procedure controls that should be in place include:

• Build any system from original, clean master copies. Boot only from original media whose write protection has always been in place, if applicable.

• Allow no media (e.g., hard/flash drives) to be used until they have been scanned on a stand-alone machine that is used for no other purpose and is not connected to the network.

• Update malware software scanning definitions/signatures frequently.

• Protect removable media against theft and hazards.

• Have vendors run demonstrations on their machines.

• Enforce a rule of not using shareware without first scanning it thoroughly for malware.

• Scan before any new software is installed because commercial software occasionally includes a Trojan horse (viruses or worms).

• Insist that field technicians scan their disks on a test machine before they use any of their disks on the system.

• Ensure the network administrator uses workstation and server anti-malware software.

• Ensure all servers are equipped with an activated current release of the malware-detection software.

• Consider encrypting files and then decrypting them before execution.

• Ensure bridge, router and gateway updates are authentic.

• Because backups are a vital element of an anti-malware strategy, ensure a sound and effective backup plan is in place. This plan should account for scanning selected backup files for malware infection once malware has been detected.

• Educate users so they will heed these policies and procedures. For example, many types of malware are propagated in the form of email attachments where the attachment, such as an executable Visual Basic script, infects the user's system upon opening the attachment. The hacker relies upon social

engineering tactics in getting the user to open the attachment.

• Review anti-malware policies and procedures at least once a year.

• Prepare a malware eradication procedure and identify a contact person.

• Develop, rehearse and maintain clear incident management procedures in the event that anti-malware software reports an infection.

Technical Controls

Technical methods of preventing malware can be implemented through hardware and software means. The following are hardware tactics that can reduce the risk of infection:

• Use boot malware protection (i.e., built-in, firmware-based malware protection).

• Use remote booting (e.g., diskless workstations).

• Use a hardware-based password.

• Protect removable media against theft and hazards.

• Ensure that insecure protocols are blocked by the firewall from external segments and the Internet.

However, anti-malware software is, by far, the most common anti-malware tool and is considered the most effective means of protecting networks and host-based computer systems against malware. Anti-malware software is both a preventive and a detective control. Unless updated periodically, antimalware software will not be an effective tool against malware.

Anti-malware software contains a number of components that address the detection of malware via scanning technologies from different angles. There are different types of anti-malware software.

Scanners look for sequences of bits called signatures that are typical of malware programs. The two primary types are:

• Malware masks or signatures—Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signatures are specific code strings that are recognized as belonging to malware. For polymorphic viruses, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.

• Heuristic scanners—Analyzes the instructions in the code being scanned and decides on the basis of statistical probability whether it could contain malicious code. Heuristic scanning results could indicate that malware may be present (i.e., possibly infected). Heuristic scanners tend to generate a high level of false-positive errors (i.e., they indicate that malware may be present when, in fact, no malware is present).

Scanners examine memory, disk-boot sectors, executables, data files and command files for bit patterns that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware-like actions. Active monitors can be problematic because they cannot distinguish between a user request and a program or malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

Integrity CRC checkers compute a binary number on a known malware-free program that is then stored in a database file. The number is called a CRC.

On subsequent scans, when that program is called to execute, it checks for changes to the files as compared to the database and reports possible infection if changes have occurred. A match means no infection; a mismatch means a change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred (i.e., it is often too late to save files). Also, CRC checkers can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware-infected and that are not recorded in the database. Integrity checkers take advantage of the fact that executable programs and boot sectors do not change often, if at all.

Behavior blockers focus on detecting potentially abnormal behavior, such as writing to the boot sector or the master boot record or making changes to executable files. Blockers can potentially detect malware at an early stage.

Most hardware-based anti-malware mechanisms are based on this concept.

Immunizers defend against malware by appending sections of themselves to files—somewhat in the same way that file malware append themselves.

Immunizers continuously check the file for changes and report changes as possible malware behavior. Other types of immunizers are focused to a specific virus and work by giving the malware the impression that the malware has already infected the computer. This method is not always practical because it is not possible to immunize files against all known malware.

Once malware has been detected by anti-malware software, an eradication program can be used to wipe the malware from the hard disk. Sometimes eradication programs can kill the malware without having to delete the infected program or data file, while other times those infected files must be deleted. Still, other programs, sometimes called inoculators, do not allow a program to be run if it contains malware.

Anti-malware Software Implementation Strategies

Organizations have to develop malware implementation strategies to effectively control and prevent the spread of malware throughout their IS

infrastructure. An important means of controlling the spread of malware is to

detect the malware at its point of entry—before it has the opportunity to cause damage. This includes everything from networks, server platforms and end-user workstations.

The user server or workstation level could include screening of software and data as they enter the machine, where anti-malware programs can be set to perform:

• Scheduled malware scans (e.g., daily, weekly, etc.)

• Manual/on-demand scans, where the malware scan is requested by the user

• Continuous/on-the-fly scanning, where files are scanned as they are processed. At the corporate network level, in cases of interconnected networks, malware scanning software is used as an integral part of firewall technologies, referred to as malware walls. Malware walls scan incoming traffic with the intent of detecting and removing malware before they enter the protected network.

• Malware walls normally work at the following levels:

• SMTP protection, to scan inbound and outbound SMTP traffic for malware in coordination with the mail server

• HTTP protection, to prevent malware-infected files from being

downloaded and to offer protection against malicious Java and ActiveX

programs

• FTP protection, to prevent infected files from being downloaded Malware walls most often are updated automatically with new malware signatures by their vendors on a scheduled basis or on an as-needed basis when dangerous, new malware emerge. Malware walls also provide facilities to log malware incidents and deal with the incident in accordance with preset rules. The presence of malware walls does not preclude the necessity for malware-detection software to be installed on computers within a network because the malware wall only addresses one channel through which malware enter the network. Malware-detection software should be loaded on all computers within the network. Malware signature files should be kept updated. The facility of automatic live update has become fairly popular and allows organizations to update the

malware scanner signature files as soon as updates are available.

For malware scanners to be acceptable and viable, they should have the following features:

• Reliability and quality in the detection of malware

• Memory resident, which is a continuous checking facility

• Efficiency, such as a reasonable working speed and usage of resources

Targeted Attacks

In a target attack, attackers target a specific organization to launch an attack in to compromise the security and steal the data. These types of attacks consist of multiple-level attacks initiated through a malware that was specifically written to get entry into an organization's systems. After the malware is installed, it creates a back door and communicates with the attacker. The attacker tries to conceal evidence of the attack to avoid detection. Using this malware, the attacker then traverses the system to understand its contents and begins to send sensitive data out of the system through a back door that the malware created. This attack continues for a

sustained period of time. After enough data is compromised, the breach is exposed.

Organizations must monitor the systems continuously to identify indicators of compromise, outgoing traffic (egress monitoring), dummy users accounts, etc. Preventive controls include baselining, hardening, exception monitoring, end-point controls, etc.

5.14 SECURITY TESTING TOOLS AND TECHNIQUES

Auditors can use different techniques for testing security. Some methods are described in the following subsections.

5.14.1 TESTING TECHNIQUES FOR COMMON SECURITY

CONTROLS

Terminal Cards and Keys

The IS auditor can take a sample of these cards or keys and attempt to gain access beyond that which is authorized. Also, the IS auditor will want to know if the security administrator followed up on any unsuccessful attempted violations.

Terminal Identification

The IS auditor can work with the network manager to get a listing of terminal addresses and locations. This list can then be used to inventory the terminals, looking for incorrectly logged, missing or additional terminals. The IS

auditor should also select a sample of terminals to ensure that they are identified in the network diagram.

Logon IDs and Passwords

To test confidentiality, the IS auditor could attempt to guess the password of a sample of employees' logon IDs (although this is not necessarily a test).

This should be done discreetly to avoid upsetting employees. The IS auditor should tour end-user and programmer work areas looking for passwords taped to the side of terminals or the inside of desk drawers. Another source of confidential information is the wastebasket. The IS auditor might consider

going through the office wastebasket looking for confidential information and passwords. Users could be asked to give their password to the IS auditor.

However, unless specifically authorized for a particular situation and supported by the security policy, users should never disclose their password.

Another way to test password strength is to analyze global configuration settings for password strength in the system application and compare this with the organization's security policy.

To test encryption, the IS auditor should work with the security administrator to attempt to view the internal password table. If viewing is possible, the contents should be unreadable. Being able to view encrypted passwords can still be dangerous. Although passwords on some systems are impossible to decipher, if an individual can obtain the encryption program, they can encrypt common passwords and look for matches. This was a method used to break into UNIX computers prior to the development of shadow password files.

Application logs should also be reviewed to ensure that passwords and logon IDs are not recorded in a clear form.

To test access authorization, the IS auditor should review a sample of access authorization documents to determine if proper authority has been provided and if the authorization was granted on a need-to-know basis. Conversely, the IS auditor should get a computer-generated report of computer access rules, take a sample to determine if the access is on a need-to-know basis, and attempt to match the sample of these rules to authorizing documents. If no written authorization is found, this indicates a breakdown in control and may warrant further review to determine the exposures and implications.

Account settings for minimizing unauthorized access should be available from most access control software or from the OS. To verify that these settings actually are working, the IS auditor can perform the following manual tests:

• To test periodic change requirements, the IS auditor can draw on his/her experiences using the system and interview a sample of users to determine if they are forced to change their password after the prescribed time interval.

• To test for disabling or deleting of inactive logon IDs and passwords, the IS

auditor should obtain a computer-generated list of active logon IDs. On a sample basis, the IS auditor should match this list to current employees, looking for logon IDs assigned to employees or consultants who are no longer with the company.

• To test for password syntax, the IS auditor should attempt to create passwords in a format that is invalid, such as too short, too long, repeated from the previous password, incorrect mix of alpha or numeric characters, or the use of inappropriate characters.

• To test for automatic logoff of unattended terminals, the IS auditor should log on to a number of terminals. The IS auditor then simply waits for the terminals to disconnect after the established time interval. Before beginning this test, the IS auditor should verify with the security administrator that this automatic logoff feature applies to all terminals.

• To test for automatic deactivation of terminals after unsuccessful access attempts, the IS auditor should attempt to log on, purposefully entering the

wrong password a number of times. The logon ID should deactivate after the established number of invalid passwords has been entered. The IS

auditor will be interested in how the security administrator reactivates the logon ID. If a simple telephone call to the security administrator with no verification of identification results in reactivation, then this function is not controlled properly.

• To test for masking of passwords on terminals, the IS auditor should log on to a terminal and observe if the password is displayed when entered.

Controls Over Production Resources

Computer access controls should extend beyond application data and transactions. There are numerous high-level utilities, macro or job control libraries, control libraries, and system software parameters for which access control should be particularly strong. Access to these libraries would provide the ability to bypass other access controls.

The IS auditor should work with the system software analyst and operations manager to determine if access is on a need-to-know basis for all sensitive production resources. Working with the security administrator, the IS auditor should determine who can access these resources and what can be done with this access.

Logging and Reporting of Computer Access Violations To test the reporting of access violations, the IS auditor should attempt to access computer transactions or data for which access is not authorized. The attempts should be unsuccessful and identified on security reports. This test should be coordinated with the data owner and security administrator to avoid violation of security regulations.

Follow-up Access Violations

To test the effectiveness and timeliness of the security administrator and data owner’s responses to reported violation attempts, the IS auditor should select a sample of security reports and look for evidence of follow-up and investigation of access violations. If such evidence cannot be found, the IS

auditor should conduct further interviews to determine why this situation exists.

Bypassing Security and Compensating Controls

This is a technical area of review. As a result, the IS auditor should work with the system software analyst, network manager, operations manager and security administrator to determine ways to bypass security. This typically includes bypass label processing, special system maintenance logon IDs, OS

exits, installation utilities and input/output (I/O) devices. Working with the security administrator, the IS auditor should determine who can access these resources and what can be done with this access. The IS auditor should determine if access is on a need-to-know/have basis or if compensating detective controls exist.

There should be restrictions and procedures of monitoring access to computer features that bypass security. Generally, only system software programmers should have access to these features:

• **Bypass label processing (BLP)**—BLP bypasses the computer reading of the file label. Because most access control rules are based on file names (labels), this can bypass access control programs.

• **System exits**—This system software feature permits the user to perform complex system maintenance, which may be tailored to a specific

environment or company. They often exist outside of the computer security system and, thus, are not restricted or reported in their use.

• **Special system logon IDs**—These logon IDs often are provided by vendors. The names can be determined easily because they are the same for all similar computer systems (i.e., system). Passwords should be changed immediately upon installation to secure the systems.

Because many of these bypassing security features can be exploited by technically sophisticated intruders, the IS auditor should also ensure that:

• All uses of these features are logged, reported and investigated by the security administrator or system software manager

• Unnecessary bypass security features are deactivated

• If possible, the bypass security features are subject to additional logical access controls

Review Access Controls and Password Administration

Access controls and password administration are reviewed to determine that:

• Procedures exist for adding individuals to the list of those authorized to have access to computer resources, changing their access capabilities and deleting them from the list.

• Procedures exist to ensure that individual passwords are not inadvertently disclosed.

• Passwords issued are of an adequate length, cannot be easily guessed and do not contain repeating characters.

• Passwords are periodically changed.

• User organizations periodically validate the access capabilities currently provided to individuals in their department.

• Procedures provide for the suspension of user identification codes (logon IDs or accounts) or the disabling of terminal, microcomputer or data entry device activity—after a particular number of security procedure violations.

5.14.2 NETWORK PENETRATION TESTS

Combinations of procedures, whereby an IS auditor uses the same techniques as a hacker, are called penetration tests, intrusion tests or ethical hacking.

These are effective methods of identifying the real-time risk to an information processing environment. During penetration testing, an auditor attempts to circumvent the security features of a system and exploits the vulnerabilities to gain access that would otherwise be unauthorized.

Scope can vary based on the terms and conditions of the client and requirements. However, from an audit risk perspective, the following should be mentioned clearly in the audit scope:

• Precise IP addresses/ranges to be tested

• Host restricted (i.e., hosts not to be tested)

• Acceptable testing techniques (i.e., social engineering, DoS/distributed denial of service [DDoS], SQL injections, etc.)

• Acceptance of proposed methodology from management

• Timing of attack simulation (i.e., business hours, off hours, etc.)

• IP addresses of the source of attack simulation (to identify between approved simulated attack and actual attack)

• Point of contact for both the penetration tester/auditor and the targeted system owner/administrator

• Handling of information collected by the penetration tester/auditor (i.e., nondisclosure agreement [NDA] or reference to standard rules of

engagement)

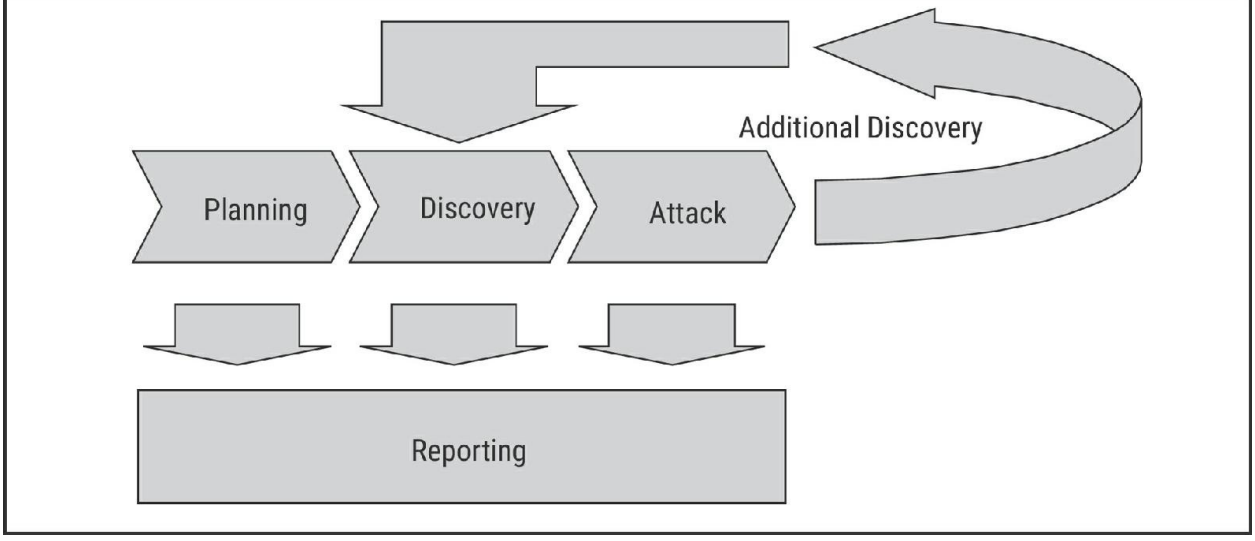
• Warning notification from penetration tester/auditor, before the simulation begins to avoid false alarms to law enforcement bodies

The different phases of penetration testing appear in **figure 5.35** and the corresponding procedures in **figure 5.36**. Penetration testing is intended to mimic an experienced hacker attacking a live site. It should only be performed by experienced and qualified professionals who are aware of the risk of undertaking such work and can limit the damage resulting from a successful break-in to a live site (e.g., avoidance of DoS attacks). It is a simulation of a real attack and maybe restricted by the law, an organization's policy and federal regulations; therefore, it is imperative to obtain management's consent in writing before finalization of the test/engagement scope.

There are several types of penetration tests depending upon the scope, objective and nature of the test. Generally accepted and common types of penetration tests are:

• **External testing**—Refers to attacks and control circumvention attempts on the target's network perimeter from outside the target's system (i.e.,

Figure 5.35—Penetration Testing Phases



usually the Internet)

• **Internal testing**—Refers to attacks and control circumvention attempts on the target from within the perimeter. The objective is to identify what would occur if the external network perimeter was successfully

compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on the network.

• **Blind testing**—Refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target's information systems. Such testing is expensive, because penetration testers have to research the target and profile it based on publicly available information only.

• **Double blind testing**—Refers to an extension of blind testing, because the administrator and security staff at the target are also not aware of the test.

Such testing can effectively evaluate the incident handling and response capability of the target.

• **Targeted testing**—Refers to attacks and control circumvention attempts on the target, while both the target's IT team and penetration testers are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they may also be provided with a limited-privilege user account to be used as a starting point to identify privilege-escalation possibilities in the system.

Figure 5.36—Penetration Testing Phases and Procedures

Planning

• Rules of engagement

• Management approval/finalization

• Adopted testing methodology

• Intrusive or nonintrusive testing

• Goals/objectives identified and agreed upon

• Timelines/deadlines agreed upon

• Milestones identified

• Assignment time tracking technique understood and communicated

• Deliverables agreed upon

• Tools collected/installed/tested in a test environment

Reconnaissance/discovery

• Network mapping

• DNS interrogation

• WHOIS queries

• Searching target’s website for information

• Searching target’s related data on search engines

• Searching target’s related data and employees on social media

(reveals system related details)

• Searching resume/curriculum vitae of target’s current and formal employees (reveals system related details)

• Packet capture/sniffing (during internal testing only)

• Host detection (Internet control message protocol [ICMP], DNS, WHOIS, PingSweep, TCP/UDP Sweep, etc.)

• Service detection (port scanning, stealth scanning, error/banner detection, etc.)

• Network topology detection (ICMP, etc.)

• OS detection (TCP stack analysis, etc.)

• Website mapping

• Web page analysis

• Unused pages/scripts

• Broken links

• Hidden links/files accessible

• Application logic/use

• Points of input error page banner grabbing

• Vulnerability classification (based on information collected in previous steps, vulnerabilities are searched on available search engines or custom-built repositories)

Some of the attack techniques are as follows:

• Directory browsing

• Show code

• Error injection

• Type and bound checks on input

Attacks

• Special character injection (meta-characters, escape characters, etc.)

• Cookie/session IDs analysis

• Authentication circumvention

• Long input

• System functions (shell escapes, etc.)

• Logic alteration (SQL injection, etc.)

• Cookie/session IDs manipulation

• Internet service exploits (bind, mdac, unicode, apache-http, statd, sadmind, etc.)

• OS exploits

• Network exploits (SYN flooding, ICMP redirects, DNS poisoning, etc.)

Furthermore, once an attack is successful, it typically follows these subprocedures of an attack phase:

• Privilege escalation—If only a user-level access was gained

previously, then the tester will attempt to obtain super-level access (i.e., root on UNIX/Linux and administrator on Windows)

• Information gathering from inside—The attacker will probe further systems on the network efficiently utilizing the compromised system as a launch pad and thereby attempt to gain access to trusted/high-risk systems.

• Installation of further attack tools inside the system—Attacker may require installation of additional tools and penetration testing software to gain further access to the resources, trusted or high-risk systems.

Reporting

This phase simultaneously occurs with the rest of the three phases.

In the planning phase, rules of engagement, written consent and test plans are developed, discussed and reported.

In the discovery phase, written logs are kept and periodic reports on the status of assignment are reported to management, as appropriate.

Following the attack phase, the vulnerabilities and weaknesses

discovered are reported with risk rating based on probability derived from ease of exploitation and impact derived from attack results or official advisories and resources from the vendor. In addition, the recommendations contain steps to mitigate the risk and to effectively rectify the weaknesses.

Although management may sponsor the activities of penetration testing, some of the associated risk includes the following:

• Penetration testing does not provide assurance that all vulnerabilities are discovered and may fail to discover significant vulnerabilities.

• Miscommunication may result in the test objectives not being achieved.

• Testing activities may inadvertently trigger escalation procedures that may not have been appropriately planned.

• Sensitive information may be disclosed, heightening the target's exposure level.

• Without proper background and qualification checks of penetration testers, the penetration tester may damage the information assets or misuse the

information gained for personal benefits.

Additionally, these techniques are becoming more popular for testing the reliability of firewall access controls. The IS auditor should be extremely careful if attempting to break into a live production system because, if successful, the IS auditor may cause the system to fail. Permission for the use of such techniques should always be obtained from top-level senior management. Permission from top-level senior management is also required to determine what other tests can be performed without informing the staff who are responsible for the monitoring and reporting of security violations (if any are aware that the attack will take places, they are likely to be more vigilant than normal).

5.14.3 THREAT INTELLIGENCE

Threat intelligence is organized, analyzed and refined information about potential or current attacks that threaten an organization provided by the service providers and some computer emergency response teams (CERTs).

The primary purpose of threat intelligence is to help an organization understand common and severe external threats, such as zero-day threats, advanced persistent threats (APTs) and exploits. The emphasis is on the attacks that are most likely to affect an organization's IT environment. Threat intelligence includes in-depth information about specific threats, including indicators of compromise (IOC), that helps the organization to protect itself from the attacks.

5.15 SECURITY MONITORING TOOLS TAND

TECHNIQUES

Monitoring, detection and logging are integral parts of security. With potential for attacks and data loss, it is necessary to monitor data and information flowing into and out of an organization. There are a number of methods and tools an organization can use to detect and log potential problems.

5.15.1 INTRUSION DETECTION SYSTEMS

An intrusion detection system (IDS) is another element of securing networks and complements firewall implementations. An IDS works with routers and firewalls by monitoring network usage anomalies. It protects an enterprise's IS resources from external and internal misuse.

An IDS operates continuously on the system, running in the background and notifying administrators when it detects a perceived threat. Broad categories of IDSs include the following:

• **Network-based IDSs**—They identify attacks within the monitored network and issue a warning to the operator. If a network-based IDS is placed between the Internet and the firewall, it will detect all the attack attempts, whether or not they enter the firewall. If the IDS is placed between a firewall and the corporate network, it will detect those attacks that enter the firewall (it will detect intruders). The IDS is not a substitute for a firewall, but it complements the function of a firewall.

• **Host-based IDSs**—They are configured for a specific environment and will monitor various internal resources of the OS to warn of a possible attack. They can detect the modification of executable programs, detect the deletion of files and issue a warning when an attempt is made to use a privileged command.

Components of an IDS are:

• Sensors that are responsible for collecting data, such as network packets, log files and system call traces

• Analyzers that receive input from sensors and determine intrusive activity

• Administration console

• User interface

Types of IDSs include:

• **Signature-based**—These IDS systems protect against detected intrusion patterns. Identified intrusive patterns are stored as signatures.

• **Statistical-based**—These systems need a comprehensive definition of the known and expected behavior of systems.

• **Neural networks**—An IDS with this feature monitors the general patterns of activity and traffic on the network and creates a database. This is similar to the statistical model but with added self-learning functionality.

Signature-based IDSs cannot detect all types of intrusions due to the limitations of the detection rules. Statistical-based systems may report many events outside of the defined normal activity but which are normal activities on the network. A combination of signature- and statistical-based models provides better protection.

Features

The features available in an IDS include:

• Intrusion detection

• Gathering evidence on intrusive activity

• Automated response (i.e., termination of connection, alarm messaging)

• Security policy

• Interface with system tools

• Security policy management

Limitations

An IDS cannot help with the following weaknesses:

• Weaknesses in the policy definition

• Application-level vulnerabilities

• Back doors into applications

• Weaknesses in identification and authentication schemes

In contrast to IDSs, which rely on signature files to identify an attack as it happens (or after), an intrusion prevention system (IPS) predicts an attack before it can take effect. It does this by monitoring key areas of a computer system and looking for bad behavior, such as worms, Trojans, spyware, malware and hackers. It complements firewall, antivirus and antispyware tools to provide complete protection from emerging threats. It is able to block new (zero-day) threats that bypass traditional security measures, because it is not reliant on identifying and distributing threat signatures or patches.

Policy

An IDS policy should establish the action to be taken by security personnel in the event that an intruder is detected.

Actions may include:

• **Terminate the access**—If there is a significant risk to the organization's data or systems, immediate termination is the usual procedure.

• **Trace the access**—If the risk to the data is low, the activity is not immediately threatening, or analysis of the entry point and attack method is desirable, the IDS can be used to trace the origin of the intrusion. This can be used to determine and correct any system weaknesses and to collect evidence of the attack which may be used in a subsequent court action.

In either case, the action required should be determined by management in advance and incorporated in a policy. This will save time when an intrusion is detected and may impact the possible data loss.

5.15.2 INTRUSION PREVENTION SYSTEMS

IPSs are closely related to IDSs and are designed to not only detect attacks, but also prevent the intended victim hosts from being affected by the attacks.

Whereas an IDS alerts or warns of an attack, requiring security personnel to act, an IPS will try to stop the attack. For example, an IPS can disconnect an

originating network or user session by blocking access to the target from the originating user account and/or IP address. Some IPSs can also reconfigure other security controls, such as a firewall or router, to block an attack. The intrusion prevention approach can be effective in limiting damage or disruption to systems that are attacked. However, as with an IDS, the IPS

must be properly configured and tuned to be effective. Threshold settings that are too high or too low will lead to limited effectiveness of the IPS. Some concerns have been raised that the IPS itself may constitute a threat, because a clever attacker could send commands to many hosts protected by an IPS to cause them to become dysfunctional. This attack could be catastrophic in environments where continuity of service is critical.

Honeypots and Honeynets

A honeypot is a software application that pretends to be a vulnerable server on the Internet and is not set up to actively protect against break-ins. A honeypot acts as a decoy system that lures hackers. The more a honeypot is targeted by an intruder, the more valuable it becomes. Although a honeypot is technically related to IDSs and firewalls, it has no real production value as an active sentinel of networks.

There are two basic types of honeypots:

• **High-interaction**—Give hackers a real environment to attack

• **Low-interaction**—Emulate production environments and provide limited information

A honeynet is a set of multiple, linked honeypots that simulate a larger network installation. Hackers infiltrate the honeynet, which allows investigators to observe the hackers' actions using a combination of surveillance technologies.

An IDS triggers a virtual alarm whenever an attacker breaches security of any networked computers. A stealthy keystroke logger watches everything the intruder types. A separate firewall cuts off the machines from the Internet anytime an intruder tries to attack another system from the honeynet.

All traffic on honeypots or honeynets are assumed to be suspicious because the systems are not meant for internal use. The information collected about these

attacks is used proactively to update vulnerabilities on an enterprise's live network.

If a honeypot is designed to be accessible from the Internet, there is a risk that external monitoring services that create lists of untrusted sites may report the organization's system as vulnerable, without knowing that the vulnerabilities belong to the honeypot and not to the system itself. Such independent reviews made public can affect the organization's reputation.

Therefore, prior to implementing a honeypot in the network, careful judgment should be exercised.

Full Network Assessment Reviews

Upon completion of penetration testing, comprehensive review of all network system vulnerabilities should occur to determine whether threats to confidentiality, integrity and availability have been identified. The following reviews should occur:

• Security policy and procedures should be reviewed to determine good practices are in place.

• The network and firewall configuration should be evaluated to ensure that they have been designed to support the security of the services being provided (e.g., screening routers, dual/multihomed host, screened subnet and DMZ proxy servers).

• The logical access controls should be evaluated to ensure that they support SoD (e.g., development vs. operation, security administration vs. audit).

• Networks have been segmented by trust levels, using appropriately configured routers.

• Determine:

– Intrusion detection software is in place.

– Filtering is being performed.

– Encryption is being used (consider VPNs/tunneling, digital signatures for

email).

– Strong forms of authentication are being used (consider use of smart cards, biometrics, for authentication to firewalls, to internal

software/hardware within the network, and to external

hardware/software).

– The firewalls have been configured properly (consider removal of all unnecessary software, addition of security and auditing software, removal of unnecessary logon IDs, disabling of unused services).

– The application- or circuit-level gateways in use are running proxy servers for all legitimate services (e.g., teletype network [Telnet], HTTP

and FTP).

– Virus scanning is being used.

– Periodic penetration testing is being completed.

– Audit logging is undertaken for all key systems (e.g., firewalls, application gateways and routers) and audit logs are copied to secure file systems (consider the use of SIEM software).

– The security administrators are keeping up to date with the latest known vulnerabilities via the organizations' vendors, their local and

international CERT, and vulnerability databases (e.g., the National Vulnerability Database operated by the NIST).

5.15.3 SECURITY INFORMATION AND EVENT

MANAGEMENT

To prepare for and identify an incident, organizations use numerous security tools, such as vulnerability assessments, firewalls and IDSs, that collect a high volume of data. An emerging solution to monitoring large amounts of data is security event management (SEM). SEM systems automatically aggregate and

correlate security event log data across multiple security devices. This allows security analysts to focus on a manageable list of critical events.

Security incidents are often made up of a series of events that occur throughout a network. By correlating data, the SEM can take many isolated events and combine them to create one single relevant security incident.

These systems use either rule-based or statistical correlation. Rule-based correlations create situation-specific rules that establish a pattern of events.

Statistical correlation uses algorithms to calculate threat levels incurred by relevant events on various IT assets.

There are a variety of SEM solutions available that provide real-time monitoring, correlation of events, notifications and console views. In addition, security information and event management (SIEM) systems take the SEM capabilities and combine them with the historical analysis and reporting features of security information management (SIM) systems.

Information security teams should periodically analyze the trends found from SEM or SIEM systems, such as attempted attack types or most frequently targeted resources. This allows the organization to investigate incidents as well as allocate appropriate resources to prevent future incidents.

One part of the organization that often uses SIEM for monitoring and detection is a security operations center (SOC). A SOC consists of an organized team created to improve the security posture of an organization and to respond to cybersecurity incidents.

5.16 INCIDENT RESPONSE MANAGEMENT

To minimize damage from security incidents and to recover and to learn from such incidents, a formal incident response capability should be established.

Figure 5.37—Incident Response Management Phases

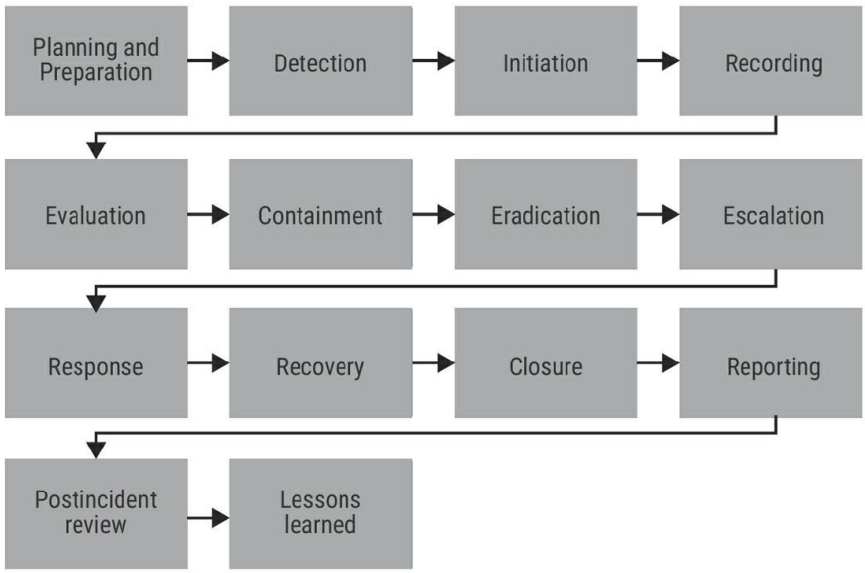


Figure 5.37 describes the phases in incident response management.

The organization and management of an incident response capability should be coordinated or centralized with the establishment of key roles and responsibilities. This should include:

• A coordinator who acts as the liaison to business process owners

• A director who oversees the incident response capability

• Managers who manage individual incidents

• Security specialists who detect, investigate, contain and recover from incidents

• Nonsecurity technical specialists who provide assistance based on subject matter expertise

• Business unit leader liaisons (legal, human resources, public relations, etc.)
Establishing this process makes employees and contractors aware of procedures for reporting the different types of incidents (e.g., security breach, threat, weakness or malfunction) that might have an impact on the security of organizational assets. Employees and contractors should be required to report any observed or suspected incidents as quickly as possible to the designated

point of contact. The organization should establish a formal disciplinary

process for dealing with those who commit security breaches, such as employees and third parties. To address incidents properly, it is necessary to collect evidence as soon as possible after the occurrence. Legal advice may be needed in the process of evidence collection and protection.

Incidents occur because vulnerabilities are not addressed properly. Incident management processes should include vulnerabilities management practices.

A postincident review phase should determine which vulnerabilities were not addressed and why, and input should be provided for improvement to the policies and procedures that are implemented to address vulnerabilities. Also, analyzing the cause of incidents may reveal errors in the risk analysis, indicating that the residual risk is higher than the calculated values and inappropriate countermeasures have been taken to reduce inherent risk.

Ideally, an organizational computer security incident response team (CSIRT) or CERT should be formed with clear lines of reporting, and responsibilities for standby support should be established. Organizational CSIRT will act as an efficient detective and corrective control. Additionally, with its members'

participation and involvement in security awareness programs, exercises and workshops, it can demonstrate a preventive control.

Organizational CSIRT should also disseminate security alerts, such as recent threats, security guidelines and security updates to the users and assist them in understanding the security risk of errors and omissions. Organizational CSIRT should act as single point of contact for all incidents and issues related to information security and should also respond to abuse reports pertaining to the network of its constituency.

An IS auditor should ensure that the CSIRT is actively involved with users to assist them in the mitigation of risk arising from security failures and also to prevent security incidents. Auditors should also ensure that there is a formal, documented plan and that it contains vulnerabilities identification, reporting and incident response procedures to common, security-related threats/issues, such as:

• Virus outbreak

• Web defacement

• Abuse notification

• Unauthorized access alert from audit trails

• Security attack alerts from intrusion detection systems (IDSs)

• Hardware/software theft

• System root compromises

• Physical security breach

• Spyware/malware/Trojans detected on personal computers (PCs)

• Fake defamatory information in media, including on websites

• Forensic investigations

Additionally, automated IDSs should be in place to notify administrators in a real-time manner of a potential incident and define a process for determining the severity of the incidents and the steps to take in high-risk situations.

5.17 EVIDENCE COLLECTION AND FORENSICS

Computer crimes are not reported in most cases because they are not detected. In many cases where computer crimes are detected, enterprises hesitate to report them because they generate a large amount of negative publicity that can affect their business. In such cases, the management of the affected enterprise seeks to fix the vulnerabilities used for the crime and resume operations. In addition, in many countries current laws are directed toward protecting physical property. It is very difficult to use such laws against computer crime. Even in jurisdictions where the laws have been updated, the investigation procedures are not always widely known, and the necessary hardware and software tools are not always available to collect the digital evidence.

In the aftermath of a computer crime, it is very important that proper procedures are used to collect evidence from the crime scene. If data and evidence is not collected in the proper manner, it could be damaged and, even if the perpetrator

is eventually identified, prosecution will not be successful in the absence of undamaged evidence. Therefore, after a computer crime, the environment and evidence must be left unaltered and specialist law enforcement officials must be called in. If the incident is to be handled in-house, the enterprise must have a suitably qualified and experienced incident

response team.

5.17.1 COMPUTER FORENSICS

Computer forensics is defined as the “process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law),” according to D.

Rodney McKemmish in Computer and Intrusion Forensics. An IS auditor may be required or asked to be involved in a forensic analysis in progress to provide expert opinion or to ensure the correct interpretation of information gathered.

Computer forensics includes activities that involve the exploration and application of methods to gather, process, interpret and use digital evidence that help to substantiate whether an incident happened, such as:

• Providing validation that an attack actually occurred

• Gathering digital evidence that can later be used in judicial proceedings Any electronic document or data can be used as digital evidence, provided there is sufficient manual or electronic proof that the contents of digital evidence are in their original state and have not been tampered with or modified during the process of collection and analysis. It is very important to preserve evidence in any situation. Most organizations are not well equipped to deal with intrusions and electronic crimes from an operational and procedural perspective, and they respond to it only when the intrusion has occurred and the risk is realized. The evidence loses its integrity and value in legal proceedings if it has not been preserved and subject to a documented chain of custody. This happens when the incident is inappropriately managed and responded to in an ad hoc manner.

For evidence to be admissible in a court of law, the chain of custody needs to be maintained professionally. The chain of evidence contains information regarding:

• Who had access to the evidence (chronological manner)

• The procedures followed in working with the evidence (e.g., disk duplication, virtual memory dump)

• Proving that the analysis is based on copies that are identical to the original

evidence (e.g., documentation, checksums or timestamps) It is important to use industry-specified good practices, proven tools and due diligence to provide reasonable assurance of the quality of evidence.

It is also important to demonstrate integrity and reliability of evidence for it to be acceptable to law enforcement authorities. For example, if the IS auditor boots a computer suspected of containing stored information that might represent evidence in a court case, the auditor cannot later deny that he/she wrote data to the hard drive because the boot sequence writes a record to the drive. This is the reason specialist tools are used to take a true copy of the drive, which is then used in the investigation.

There are four major considerations in the chain of events for evidence in computer forensics:

• **Identify**—Refers to the identification of information that is available and might form the evidence of an incident.

• **Preserve**—Refers to the practice of retrieving identified information and preserving it as evidence. The practice generally includes the imaging of original media in presence of an independent third party. The process also requires being able to document chain-of-custody so that it can be established in a court of law.

• **Analyze**—Involves extracting, processing and interpreting the evidence.

Extracted data could be unintelligible binary data after it has been processed and converted into human readable format. Interpreting the data requires an in-depth knowledge of how different pieces of evidence may fit together. The analysis should be performed using an image of media and not the original.

• **Present**—Involves a presentation to the various audiences, such as management, attorneys, court, etc. Acceptance of the evidence depends on the manner of presentation (because it should be convincing),

qualifications of the presenter and credibility of the process that is used to preserve and analyze the evidence.

The IS auditor should consider key elements of computer forensics during audit planning. These key elements are described in the following

subsections.

Data Protection

To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocols to inform appropriate parties that electronic evidence will be sought and to not destroy it by any means.

Infrastructure and processes for incident response and handling should be in place to permit an effective response and forensic investigation if an event or incident occurs.

Data Acquisition

All information and data required should be transferred into a controlled location. This includes all types of electronic media, such as fixed disk drives and removable media. Each device must be checked to ensure that it is write-protected. This may be achieved by using a device known as a write-blocker.

It is also possible to get data and information from witnesses or related parties by recorded statements.

By examining volatile data, investigators can determine what is currently happening on a system. This kind of data includes open ports, open files, active processes, user logons and other data present in RAM. This information is lost when the computer is shut down.

Imaging

Imaging is a process that allows one to obtain a bit-for-bit copy of data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by

sector.

With appropriate tools, it is sometimes possible to recover destroyed information (erased even by reformatting) from the disk's surface.

Extraction

This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made.

The extraction process could include different sources, such as system logs, firewall logs, IDS logs, audit trails and network management information.

Interrogation

Interrogation is used to obtain prior indicators or relationships, including telephone numbers, IP addresses and names of individuals, from extracted data.

Ingestion/Normalization

This process converts the information extracted to a format that can be understood by investigators. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tools. It is possible to create relationships from data by extrapolation, using techniques, such as fusion, correlation, graphing, mapping or time lining, which could be used in the construction of the investigation's hypothesis.

Reporting

The information obtained from computer forensics has limited value when it is not collected and reported in the proper way.

When an IS auditor writes the report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusions were made from this analysis.

The report should achieve the following goals (from Mandia, Kevin; Matt Pepe; Chris Prosise; Incident Response & Computer Forensics, 2nd Edition, McGraw

Hill/Osborne, USA, 2003):

• Accurately describe the details of an incident

• Be understandable to decision-makers

• Be able to withstand a barrage of legal scrutiny

• Be unambiguous and not open to misinterpretation

• Be easily referenced

• Contain all information required to explain conclusions reached

• Offer valid conclusions, opinions or recommendations when needed

• Be created in a timely manner

The report should also identify the organization, sample reports and restrictions on circulation (if any) and include any reservations or qualifications that the IS auditor has with respect to the assignment.

5.17.2 PROTECTION OF EVIDENCE AND CHAIN OF CUSTODY

The evidence of a computer crime exists in the form of log files, file time stamps, contents of memory, etc. Rebooting the system or accessing files could result in such evidence being lost, corrupted or overwritten. Therefore, one of the first steps taken should be copying one or more images of the attacked system.

Memory content should also be dumped to a file before rebooting the system.

Any further analysis must be performed on an image of the system and on copies of the memory dumped—not on the original system in question.

In addition to protecting the evidence, it is also important to preserve the chain of custody. Chain of custody refers to documenting, in detail, how evidence is handled and maintained, including its ownership, transfer and modification. This is necessary to satisfy legal requirements that mandate a high level of confidence

regarding the integrity of evidence.

CASE STUDY

Spectertainment is a company dedicated to the production and distribution of video clips specializing in jazz music. Born in the Internet era, the company has actively supported the use of laptops and tablets so staff easily work remotely. They can access the company databases through the Internet and provide online information to customers. This decision to support remote work has resulted in an increase in productivity and high morale among employees who are allowed to work up to two days a week from home.

Based on written procedures and a training course, employees learn security procedures to avoid the risk of unauthorized access to company data.

Employees' access to the company data includes using logon IDs and passwords to the application server through a VPN. Initial passwords are assigned by the security administrator. When the employee logs on for the first time, the system forces a password change to improve confidentiality.

Management is currently considering ways to improve security protection for remote access by employees.

1.

Which of the following would be of **MOST** concern to an IS auditor reviewing a VPN implementation? Computers on the network that are located:

A. on the enterprise's internal network.

B. at the backup site.

C. in employees' homes.

D. at the enterprise's remote offices.

2.

Which of the following levels provides a higher degree of protection in applying access control software to avoid unauthorized access risk?

A. Network and OS level

B. Application level

C. Database level

D. Log file level

3.

When an employee notifies the company that he/she has forgotten

his/her password, what should be done **FIRST** by the security administrator?

A. Allow the system to randomly generate a new password

B. Verify the user’s identification through a challenge/response system

C. Provide the employee with the default password and explain that it should be changed as soon as possible

D. Ask the employee to move to the administrator terminal to generate a new password in order to assure confidentiality

Spectertainment asks its IS auditor to review its new virtual private network implementation to accommodate the increase in remote work. The auditor discovers that the organization needed to enable remote access to one of its servers for remote maintenance purposes. Firewall policy did not allow any external access to the internal systems. Therefore, it was decided to install a modem on that server and to activate the remote access service to permit dial-up access. To mitigate any vulnerabilities associated with dial-up modems, a policy has been implemented to manually power on the modem only when the third party was requesting access to the server and powered off by the company’s system administrator when the access is no longer needed.

Because more and more systems are being maintained remotely, the company is asking an IS auditor to evaluate the current risk of the existing solution and to propose the best strategy for addressing future connectivity requirements.

4.

What test is **MOST** important for the IS auditor to perform as part of the review of dial-up access controls?

A. Dial the server from authorized and unauthorized telephone lines B. Determine bandwidth requirements of remote maintenance and the

maximum line capacity

C. Check if the availability of the line is guaranteed to allow remote access any time

D. Check if call back is not used and the cost of calls is charged to the third party

5.

What is the **MOST** significant risk that the IS auditor should evaluate regarding the existing remote access practice?

A. Modem is not powered on/off whenever is needed

B. A nondisclosure agreement was not signed by the third party

C. Data exchanged over the line is not encrypted

D. Firewall controls are bypassed

6.

Which of the following recommendations is **MOST** likely to reduce the current level of remote access risk?

A. Maintain an access log with the date and time when the modem was powered on/off

B. Encrypt the traffic over the telephone line

C. Migrate the dial-up access to an Internet VPN solution

D. Update firewall policies and implement an IDS

7.

What control should be implemented to prevent an attack on the

internal network being initiated though an Internet VPN connection?

A. Firewall rules are periodically reviewed

B. All VPNs terminate at a single concentrator

C. An IPS capable to analyze encrypted traffic is implemented

D. Antivirus software is installed on all production servers

ANSWER TO CASE STUDY QUESTIONS

1.

A.

On an enterprise's internal network, there should be security

policies and controls in place to detect and halt an outside attack that uses an internal machine as a staging platform. Therefore,

this would not be the biggest concern to the IS audit.

B.

Computers at the backup site are subject to the corporate security policy and, therefore, are not high-risk computers.

C.

VPN offers a secure connection between the remote PC and

the corporate network. VPN does not, however, protect the

remote PC from outside attack (such as from the Internet). If the remote PC is compromised, a malicious actor can use that

entry point of the compromised remote PC to enter the

corporate network (lateral movement).

D.

Computers on the network that are at the enterprise's remote

offices, perhaps with different IS and security employees who

have different ideas about security, are riskier than computers in the main office or backup site, but obviously less risky than home computers.

2.

A.

The greatest degree of protection in applying access control

software against internal and external users' unauthorized

access is at the network and platform/OS levels. These

systems are also referred to as general support systems, and

they make up the primary infrastructure on which

applications and database systems will reside.

B.

The application level is part of the infrastructure made up by the general support systems, supported by the network and OS level.

C.

The database level is part of the infrastructure made up by the

general support systems, supported by the network and OS level.

D.

The log file level is part of the infrastructure made up by the

general support systems, supported by the network and OS level.

3.

A.

When an employee notifies that he/she has forgotten his/her

password, the security administrator should start a password

process generation procedure only after verifying the user’s

identification using a challenge/response system or similar

procedure.

B.

A challenge/response system or similar procedure should be

the first stem in verifying a user’s identity. To verify, it is advised that the security administrator should return the

user’s call after verifying his/her extension or calling his/her supervisor for verification.

C.

Before an employee is provided with the default password, their

identity should be first verified using a challenge/response system or similar procedure.

D.

Before any further action is taken, the user’s identity must be

verified. A new password should not be generated until this is

confirmed, regardless of the security of the terminal.

4.

A.

Dial-up access should be possible only from authorized

telephone lines as a preventive control for unauthorized

access when logon credentials are compromised or misused by

third-party personnel. Initiating the connection by the server to an authorized phone number using the callback feature

would be one implementation of this requirement.

B.

Determining bandwidth requirements addresses performance

issues but not access control issues.

C.

Checking line availability addresses performance issues but not

access control issues.

D.

Checking that call back is not used and the cost of calls are

charged back to the third party addresses performance issues but not access control issues.

5.

A.

The modem not powered on/off whenever needed is a type of

risk to be considered by the IS auditor, but concerns only the

server being maintained remotely, and not the entire internal

system.

B.

An unsigned nondisclosure agreement is a type of risk to be

considered by the IS auditor, but concerns only the server being maintained remotely, and not the entire internal system.

C.

Unencrypted data is a type of risk to be considered by the IS

auditor, but concerns only the server being maintained remotely, and not the entire internal system.

D.

The company’s security infrastructure relies on controls

implemented on the firewall. The fact that someone from the outside can connect directly to an internal system, bypassing firewall rules, could expose the internal network to the third party, thereby facilitating unauthorized access.

6.

A.

Maintaining an access log will address punctual issues but will

not reduce the level of risk.

B.

Encrypting traffic will address punctual issues but will not reduce the level of risk.

C.

Using an Internet VPN solution will eliminate the

vulnerabilities of the dial-up access, such as lack of encryption and bypassing firewall controls.

D.

Updating firewall policies and implementing an IDS will have no

effect since security infrastructure controls are bypassed by the direct dial-up access.

7.

A.

A firewall rules review and ending all VPNs in a single

concentrator will prevent unauthorized connections to the internal network, but this will not prevent an attack occurring through an authorized VPN connection.

B.

Having all VPNs terminate at a single connector will not

necessarily prevent attacks from occurring.

C.

An IPS should be able to analyze the encrypted traffic of the VPN connection to determine potential attacks.

D.

Antivirus software will prevent contamination by computer

viruses, but the internal system is still vulnerable to many other threats.

APPENDIX A: CISA EXAM GENERAL

INFORMATION

ISACA is a professional membership association composed of individuals interested in IS audit, assurance, control, security and governance. The CISA Certification Working Group is responsible for establishing policies for the CISA certification program and developing the exam.

Note: Because information regarding the CISA examination may change, please refer to www.isaca.org/certification for the most current information.

REQUIREMENTS FOR CERTIFICATION

The CISA designation is awarded to those individuals who have met the following requirements:

(1) A passing score on the CISA exam

(2) Submitting verified evidence of IS auditing, control, assurance or security experience

(3) Abiding by the *Code of Professional Ethics*

(4) Abiding by the continuing professional education policy

(5) Abiding by the IS Auditing Standards as adopted by ISACA.

SUCCESSFUL COMPLETION OF THE CISA EXAM

The exam is open to all individuals who wish to take it. Successful exam candidates are not certified until they apply for certification (and demonstrate that they have met all requirements) and receive approval from ISACA.

EXPERIENCE IN IS AUDITING, CONTROL AND

SECURITY

A minimum of five years professional IS auditing, control, assurance and security work experience is required for certification. Please refer to

www.isaca.org/certification for a list of experience waivers.

Experience must have been gained within the 10-year period preceding the application date for certification or within five years from the date of initially

passing the exam. A completed application for certification must be submitted within five years from the passing date of the CISA exam. All experience must be independently verified with employers.

DESCRIPTION OF THE EXAM

The CISA Certification Working Group oversees the development of the exam and ensures the currency of its content. Questions for the CISA exam are developed through a multitiered process that is designed to enhance the ultimate quality of the exam.

The purpose of the exam is to evaluate a candidate's knowledge and experience in conducting IS audits and reviews. The exam consists of 150

multiple-choice questions, administered during a four-hour session.

REGISTRATION FOR THE CISA EXAM

The CISA exam is administered on a continuous basis at qualifying test sites.

Please refer to the *ISACA Exam Candidate Information Guide* at

www.isaca.org/examguide for specific exam registration information, including registration, scheduling and languages, and important key information for exam day. Exam registrations can be made online at

www.isaca.org/examreg.

CISA PROGRAM ACCREDITATION RENEWED UNDER

ISO/IEC 17024:2012

The American National Standards Institute (ANSI) has voted to continue the accreditation for the CISA, CISM, CGEIT and CRISC certifications, under ISO/IEC 17024:2012, General Requirements for Bodies Operating

Certification Systems of Persons. ANSI, a private, nonprofit organization, accredits other organizations to serve as third-party product, system and personnel certifiers.

ISO/IEC 17024 specifies the requirements to be followed by organizations certifying individuals against specific requirements. ANSI describes ISO/IEC

17024 as “expected to play a prominent role in facilitating global standardization of the certification community, increasing mobility among countries, enhancing public safety, and protecting consumers.”

ANSI’s accreditation:

• Promotes the unique qualifications and expertise that ISACA’s

certifications provide

• Protects the integrity of the certifications and provides legal defensibility

• Enhances consumer and public confidence in the certifications and the people who hold them

• Facilitates mobility across borders or industries

Accreditation by ANSI signifies that ISACA’s procedures meet the ANSI essential requirements for openness, balance, consensus and due process.

With this accreditation, ISACA anticipates that significant opportunities for CISAs, CISMs, CGEITs and CRISCs will continue to open in the United States and around the world.

SCHEDULING THE EXAM

The CISA exam can be scheduled directly from your My ISACA profile.

Please see the *Exam Candidate Information Guide* at

www.isaca.org/examguide for complete instructions. Exams can be scheduled for any available time slot. Exams may be rescheduled a minimum of 48

hours prior to the originally scheduled appointment. If you are within 48

hours of your original appointment, you must take your exam or forfeit the exam registration fee.

SITTING FOR THE EXAM

Prior to the day of the exam, make sure you:

• Locate the test center and confirm the start time

• Plan to arrive 15 minutes prior to exam start time

• Plan to store personal belongings

• Review the exam day rules

You must present an acceptable form of identification (ID) to enter the testing center. Please see the *Exam Candidate Information Guide* at

www.isaca.org/examguide for acceptable forms of ID.

You are prohibited from bringing the following into the test center:

• Reference materials, paper, notepads or language dictionaries

• Calculators

• Any type of communication, surveillance or recording devices, such as:

– Mobile phones

– Tablets

– Smart watches or glasses

– Mobile devices

• Baggage of any kind including handbags, purses or briefcases

• Weapons

• Tobacco products

• Food or beverages

• Visitors

If exam candidates are viewed with any such communication, surveillance or recording devices during the exam administration, their exam will be voided, and they will be asked to immediately leave the exam site.

Personal items brought to the testing center must be stored in a locker or other designated area until the exam is completed and submitted.

Avoid activities that would invalidate your test score, such as:

• Creating a disturbance

• Giving or receiving help; using notes, papers or other aids

• Attempting to take the exam for someone else

• Possession of communication, surveillance or recording device, including

but not limited to cell phones, tablets, smart glasses, smart watches and mobile devices., during the exam administration

• Attempting to share test questions or answers or other information contained in the exam (as such are the confidential information of ISACA); including sharing test questions subsequent to the exam

• Leaving the testing area without authorization (These individuals will not be allowed to return to the testing room.)

• Accessing items stored in the personal belongings area before the completion of the exam

BUDGETING YOUR TIME

The exam is administered over a four-hour period. This allows for a little over 1.5 minutes per question. Therefore, it is advisable that candidates pace themselves to complete the entire exam. To do so, candidates should complete an average of 38 questions per hour.

GRADING THE EXAM

Candidate scores are reported as a scaled scored. A scaled score is a conversion of a candidate's raw score on an exam to a common scale. ISACA uses and reports scores on a common scale from 200 to 800.

A candidate must receive a score of 450 or higher to pass the exam. A score of 450 represents a minimum consistent standard of knowledge as established by ISACA's CISA Certification Working Group. A candidate receiving a passing score may then apply for certification if all other requirements are met.

Passing the exam does not grant the CISA designation. To become a CISA, each candidate must complete all requirements, including submitting an application and receiving approval for certification.

The CISA examination contains some questions that are included for research and analysis purposes only. These questions are not separately identified, and the candidate's final score will be based only on the common scored

questions. There are various versions of each exam but only the common questions are scored for your results.

A candidate receiving a score less than 450 is not successful and can retake the exam by registering and paying the appropriate exam fee. To assist with future study, the result letter each candidate receives will include a score analysis by content area.

Candidates will receive a preliminary score on screen immediately following the completion of their exam. **Their official score will be emailed to them and available online within 10 working days.** Question-level results cannot be provided.

To become CISA-certified, candidates must pass the CISA exam, and must complete and submit an application for certification (and must receive confirmation from ISACA that the application is approved). The application is available on the ISACA website at *www.isaca.org/cisaapp*. After the application is approved, the applicant will be sent confirmation of the approval. The candidate is not CISA-certified and cannot use the CISA designation, until the candidate's application is approved. A processing fee must accompany CISA applications for certification.

Candidates receiving a failing score on the exam may request a rescoring of their

exam within 30 days following the release of the exam results. All requests must include a candidate’s name, exam identification number and candidate mailing address. A fee of US $75 must accompany this request.

APPENDIX B: CISA 2019 JOB

PRACTICE

DOMAIN 1—THE PROCESS OF AUDITING

INFORMATION SYSTEMS

(21 PERCENT)

A. Planning

1.

IS Audit Standards, Guidelines, and Codes of Ethics

2.

Business Processes

3.

Types of Controls

4.

Risk-Based Audit Planning

5.

Types of Audits and Assessments

B. Execution

1.

Audit Project Management

2.

Sampling Methodology

3.

Audit Evidence Collection Techniques

4.

Data Analytics

5.

Reporting and Communication Techniques

DOMAIN 2—GOVERNANCE AND MANAGEMENT OF IT

(17 PERCENT)

A. IT Governance

1.

IT Governance and IT Strategy

2.

IT-Related Frameworks

3.

IT Standards, Policies, and Procedures

4.

Organizational Structure

5.

Enterprise Architecture

6.

Enterprise Risk Management

7.

Maturity Models

8.

Laws, Regulations, and Industry Standards affecting the Organization **B. IT Management**

1.

IT Resource Management

2.

IT Service Provider Acquisition and Management

3.

IT Performance Monitoring and Reporting

4.

Quality Assurance and Quality Management of IT

DOMAIN 3—INFORMATION SYSTEMS ACQUISITION,

DEVELOPMENT, AND IMPLEMENTATION (12

PERCENT)

A. Information Systems Acquisition and Development

1.

Project Governance and Management

2.

Business Case and Feasibility Analysis

3.

System Development Methodologies

4.

Control Identification and Design

B. Information Systems Implementation

1.

Testing Methodologies

2.

Configuration and Release Management

3.

System Migration, Infrastructure Deployment, and Data Conversion 4.

Post-implementation Review

DOMAIN 4—INFORMATION SYSTEMS OPERATIONS

AND BUSINESS RESILIENCE

(23 PERCENT)

A. Information Systems Operations

1.

Common Technology Components

2.

IT Asset Management

3.

Job Scheduling and Production Process Automation

4.

System Interfaces

5.

End-User Computing

6.

Data Governance

7.

Systems Performance Management

8.

Problem and Incident Management

9.

Change, Configuration, Release, and Patch Management

10. IT Service Level Management

11. Database Management

B. Business Resilience

1.

Business Impact Analysis (BIA)

2.

System Resiliency

3.

Data Backup, Storage, and Restoration

4.

Business Continuity Plan (BCP)

5.

Disaster Recovery Plans (DRP)

DOMAIN 5—PROTECTION OF INFORMATION ASSETS

(27 PERCENT)

A. Information Asset Security and Control

1.

Information Asset Security Frameworks, Standards, and Guidelines 2.

Privacy Principles

3.

Physical Access and Environmental Controls

4.

Identity and Access Management

5.

Network and End-Point Security

6.

Data Classification

7.

Data Encryption and Encryption-Related Techniques

8.

Public Key Infrastructure (PKI)

9.

Web-Based Communication Techniques

10. Virtualized Environments

11. Mobile, Wireless, and Internet-of-Things (IoT) Devices

B. Security Event Management

1.

Security Awareness Training and Programs

2.

Information System Attack Methods and Techniques

3.

Security Testing Tools and Techniques

4.

Security Monitoring Tools and Techniques

5.

Incident Response Management

6.

Evidence Collection and Forensics

SUPPORTING TASKS

1.

Plan audit to determine whether information systems are protected, controlled, and provide value to the organization.

2.

Conduct audit in accordance with IS audit standards and a risk-based IS

audit strategy.

3.

Communicate audit progress, findings, results, and recommendations to stakeholders.

4.

Conduct audit follow-up to evaluate whether risk has been sufficiently addressed.

5.

Evaluate the IT strategy for alignment with the organization’s strategies and objectives.

6.

Evaluate the effectiveness of IT governance structure and IT

organizational structure.

7.

Evaluate the organization’s management of IT policies and practices.

8.

Evaluate the organization’s IT policies and practices for compliance with

regulatory and legal requirements.

9.

Evaluate IT resource and portfolio management for alignment with the organization’s strategies and objectives.

10. Evaluate the organization’s risk management policies and practices.

11. Evaluate IT management and monitoring of controls.

12. Evaluate the monitoring and reporting of IT key performance indicators (KPIs).

13. Evaluate the organization’s ability to continue business operations.

14. Evaluate whether the business case for proposed changes to information systems meet business objectives.

15. Evaluate whether IT supplier selection and contract management processes align with business requirements.

16. Evaluate the organization’s project management policies and practices.

17. Evaluate controls at all stages of the information systems development life cycle.

18. Evaluate the readiness of information systems for implementation and migration into production.

19. Conduct post-implementation review of systems to determine whether project deliverables, controls, and requirements are met.

20. Evaluate whether IT service management practices align with business requirements.

21. Conduct periodic review of information systems and enterprise architecture.

22. Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization’s objectives.

23. Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization’s objectives.

24. Evaluate database management practices.

25. Evaluate data governance policies and practices.

26. Evaluate problem and incident management policies and practices.

27. Evaluate change, configuration, release, and patch management policies and practices.

28. Evaluate end-user computing to determine whether the processes are effectively controlled.

29. Evaluate the organization’s information security and privacy policies and practices.

30. Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded.

31. Evaluate logical security controls to verify the confidentiality, integrity, and availability of information.

32. Evaluate data classification practices for alignment with the organization’s policies and applicable external requirements.

33. Evaluate policies and practices related to asset life cycle management.

34. Evaluate the information security program to determine its effectiveness and alignment with the organization’s strategies and objectives.

35. Perform technical security testing to identify potential threats and vulnerabilities.

36. Utilize data analytics tools to streamline audit processes.

37. Provide consulting services and guidance to the organization in order to improve the quality and control of information systems.

38. Identify opportunities for process improvement in the organization’s IT

policies and practices.

39. Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.

GLOSSARY

Note: Glossary terms are provided for reference within the CISA Review Manual. Because term definitions may evolve due to the changing

technological environment, please see www.isaca.org/glossary for the most up-to-date terms and definitions.

A

Abend—An abnormal end to a computer job; termination of a task prior to its completion because of an error condition that cannot be resolved by recovery facilities while the task is executing

Acceptable use policy—A policy that establishes an agreement between users and the enterprise and defines for all parties' the ranges of use that are approved before gaining access to a network or the Internet

Access control—The processes, rules and deployment mechanisms that control access to information systems, resources and physical access to premises

Access control list (ACL)—An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals. Also referred to as access control tables.

Access control table—An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals

Access method—The technique used for selecting records in a file, one at a time, for processing, retrieval or storage. The access method is related to, but distinct from, the file organization, which determines how the records are stored.

Access path—The logical route an end user takes to access computerized

information. Typically, it includes a route through the operating system,

telecommunications software, selected application software and the access control system.

Access rights—The permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy

Access servers—Provides centralized access control for managing remote access dial-up services

Address—Within computer storage, the code used to designate the location of a specific piece of data

Address space—The number of distinct locations that may be referred to with the machine address. For most binary machines, it is equal to 2n, where n is the number of bits in the machine address.

Addressing—The method used to identify the location of a participant in a network. Ideally, addressing specifies where the participant is located rather than who they are (name) or how to get there (routing).

Administrative controls—The rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies

Adware—A software package that automatically plays, displays or downloads advertising material to a computer after the software is installed on it or while the application is being used. In most cases, this is done without any notification to the user or without the user's consent. The term adware may also refer to software that displays advertisements, whether or not it does so with the user's consent; such programs display advertisements as an alternative to shareware registration fees. These are classified as adware in the sense of advertising supported software, but not as spyware. Adware in this form does not operate surreptitiously or mislead the user and provides the user with a specific service.

Alpha—The use of alphabetic characters or an alphabetic character string
Alternative routing—A service that allows the option of having an alternate route to complete a call when the marked destination is not available. In signaling, alternate routing is the process of allocating substitute routes for a given signaling traffic stream in case of failure(s) affecting the normal signaling

links or routes of that traffic stream.

American Standard Code for Information Interchange—See ASCII.

Analog—A transmission signal that varies continuously in amplitude and time and is generated in wave formation. Analog signals are used in telecommunications.

Anonymous File Transfer Protocol (FTP)—A method for downloading public files using the File Transfer Protocol. Anonymous FTP is called anonymous because users do not need to identify themselves before accessing files from a particular server. In general, users enter the word

"anonymous" when the host prompts for a username; anything can be entered for the password, such as the user's email address or simply the word

"guest." In many cases, an anonymous FTP site will not even prompt users for a name and password.

Antivirus software—An application software deployed at multiple points in an IT architecture. It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected.

Applet—A program written in a portable, platform independent computer language such as Java, JavaScript or Visual Basic. An applet is usually embedded in a Hypertext Markup Language (HTML) page downloaded from web servers and then executed by a browser on client machines to run any web-based application (e.g., generate web page input forms, run audio/video programs, etc.). Applets can only perform a restricted set of operations, thus preventing, or at least minimizing, the possible security compromise of the host computers. However, applets expose the user's machine to risk if not properly controlled by the browser, which should not allow an applet to

access a machine's information without prior authorization of the user.

Application—A computer program or set of programs that perform the processing of records for a specific function. Contrasts with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort.

Application controls—The policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved

Application layer—In the Open Systems Interconnection (OSI) communications model, the application layer provides services for an application program to ensure that effective communication with another application program in a network is possible. The application layer is not the application that is doing the communication; a service layer that provides these services.

Application program—A program that processes business data through activities such as data entry, update or query. Contrasts with systems programs, such as an operating system or network control program, and with utility programs such as copy or sort.

Application programming—The act or function of developing and maintaining applications programs in production

Application programming interface (API)—A set of routines, protocols and tools referred to as building blocks used in business application software development. A good API makes it easier to develop a program by providing all the building blocks related to functional characteristics of an operating system that applications need to specify, for example, when interfacing with the operating system (e.g., provided by Microsoft Windows, different versions of UNIX). A programmer uses these APIs in developing

applications that can operate effectively and efficiently on the platform chosen.

Application software tracing and mapping—Specialized tools that can be

used to analyze the flow of data through the processing logic of the application software and document the logic, paths, control conditions and processing sequences. The command language or job control statements, and programming language can be analyzed. This technique includes

program/system: mapping, tracing, snapshots, parallel simulations and code comparisons.

Arithmetic logic unit (ALU)—The area of the central processing unit that performs mathematical and analytical operations

Artificial intelligence—Advanced computer systems that can simulate human capabilities, such as analysis, based on a predetermined set of rules **ASCII**—Representing 128 characters, the American Standard Code for Information Interchange (ASCII) code normally uses 7 bits. However, some variations of the ASCII code set allow 8 bits. This 8-bit ASCII code allows 256 characters to be represented.

Assembler—A program that takes as input a program written in assembly language and translates it into machine code or machine language **Asymmetric key (public key)**—A cipher technique in which different cryptographic keys are used to encrypt and decrypt a message (See public key encryption)

Asynchronous Transfer Mode (ATM)—A high-bandwidth low-delay switching and multiplexing technology that allows integration of real-time voice, video and data. It is a data link layer protocol. ATM is a protocol-independent transport mechanism. It allows high-speed data transfer rates at up to 155 Mbit/s. The acronym ATM should not be confused with the alternate usage for ATM, which refers to an automated teller machine.

Asynchronous transmission—Character-at-a-time transmission **Attribute sampling**—An audit technique used to select items from a population for audit testing purposes based on selecting all those items that have certain attributes or characteristics (such as all items over a certain size)

Audit evidence—The information used to support the audit opinion **Audit objective**—The specific goal(s) of an audit. These often center on substantiating the existence of internal controls to minimize business risk.

Audit plan—1. A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members to obtain

sufficient appropriate audit evidence to form an opinion. Includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work, and topics such as budget, resource allocation, schedule dates, type of report, its intended audience and other general aspects of the work 2. A high-level description of the audit work to be performed in a certain period of time

Audit program—A step-by-step set of audit procedures and instructions that should be performed to complete an audit

Audit risk—The probability that information or financial reports may contain material errors and that the auditor may not detect an error that has occurred

Audit trail—A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source **Authentication**—The act of verifying the identity of a user and the user's eligibility to access computerized information. Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.

B

Backbone—The main communications channel of a digital network. The part of the network that handles the major traffic. Employs the highest-speed transmission paths in the network and may also run the longest distances.

Smaller networks are attached to the backbone, and networks that connect directly to the end user or customer are called access networks. A backbone

can span a geographic area of any size, from a single building to an office complex, to an entire country. Or, it can be as small as a backplane in a single cabinet.

Backup—Files, equipment, data and procedures available for use in the event of a failure or loss, if the originals are destroyed or out of service **Badge**—A card or other device that is presented or displayed to obtain access to an otherwise restricted facility, as a symbol of authority (e.g., police) or as a simple means of identification. Also used in advertising and publicity.

Balanced scorecard (BSC)—Developed by Robert S. Kaplan and David P.

Norton as a coherent set of performance measures organized into four categories that includes traditional financial measures, but adds customer, internal business process, and learning and growth perspectives

Bandwidth—The range between the highest and lowest transmittable frequencies. It equates to the transmission capacity of an electronic line and is expressed in bytes per second or Hertz (cycles per second).

Bar code—A printed machine-readable code that consists of parallel bars of

varied width and spacing

Base case—A standardized body of data created for testing purposes. Users normally establish the data. Base cases validate production application systems and test the ongoing accurate operation of the system.

Baseband—A form of modulation in which data signals are pulsed directly on the transmission medium without frequency division and usually utilize a transceiver. The entire bandwidth of the transmission medium (e.g., coaxial cable) is utilized for a single channel.

Batch control—Correctness checks built into data processing systems and applied to batches of input data, particularly in the data preparation stage.

There are two main forms of batch controls: sequence control, which involves consecutively numbering the records in a batch so that the presence of each record can be confirmed, and control total, which is a total of the

values in selected fields within the transactions.

Batch processing—The processing of a group of transactions at the same time. Transactions are collected and processed against the master files at a specified time.

Baud rate—The rate of transmission for telecommunications data, expressed in bits per second (bps)

Bayesian filter—A method often employed by antispam software to filter spam based on probabilities. The message header and every word or number are each considered a token and given a probability score. Then the entire message is given a spam probability score. A message with a high score will be flagged as spam and discarded, returned to its sender or put in a spam directory for further review by the intended recipient.

Benchmarking—A systematic approach to comparing organization performance against peers and competitors in an effort to learn the best ways of conducting business. Examples include benchmarking of quality, logistic efficiency and various other metrics.

Binary code—A code whose representation is limited to 0 and 1

Biometrics—A security technique that verifies an individual's identity by analyzing a unique physical attribute such as a handprint

Black box testing—A testing approach that focuses on the functionality of the application or product and does not require knowledge of the code intervals

Bridge—A device that connects two similar networks together **Broadband**—Multiple channels are formed by dividing the transmission medium into discrete frequency segments. Broadband generally requires the use of a modem.

Brouters—Devices that perform the functions of both a bridge and a router.

A brouter operates at both the data link and the network layers. It connects same data-link-type local area network (LAN) segments and different data-link ones, which is a significant advantage. Like a bridge, it forwards packets based on the data-link layer address to a different network of the same type.

Also, whenever required, it processes and forwards messages to a different data-link-type network based on the network protocol address. When connecting same data-link type networks, it is as fast as a bridge and is able to connect different data-link type networks.

Buffer—Memory reserved to temporarily hold data to offset differences between the operating speeds of different devices, such as a printer and a computer. In a program, buffers are reserved areas of random access memory (RAM) that hold data while they are being processed.

Bus—Common path or channel between hardware devices. Can be located between components internal to a computer or between external computers in a communications network.

Bus configuration—All devices (nodes) are linked along one communication line where transmissions are received by all attached nodes.

This architecture is reliable in very small networks and is easy to use and understand. This configuration requires the least amount of cable to connect the computers together and, therefore, is less expensive than other cabling arrangements. It is also easy to extend, and two cables can be easily joined with a connector to make a longer cable for more computers to join the network. A repeater can also be used to extend a bus configuration.

Business case—Documentation of the rationale for making a business investment, used to support a business decision on whether to proceed with the investment and as an operational tool to support management of the investment through its full economic life cycle

Business continuity plan (BCP)—A plan used by an organization to respond to disruption of critical business processes. Depends on the contingency plan for restoration of critical systems.

Business impact analysis (BIA)—A process to determine the impact of

losing the support of any resource. The BIA assessment study establishes the escalation of that loss over time. It is predicated on the fact that senior management, when provided reliable data to document the potential impact of a lost resource, can make the appropriate decision.

Business process reengineering (BPR)—The thorough analysis and significant redesign of business processes and management systems to establish a better performing structure, more responsive to the customer base and market conditions, while yielding material cost savings

Business risk—A probable situation with uncertain frequency and magnitude of loss (or gain)

Bypass label processing (BLP)—A technique of reading a computer file while bypassing the internal file/data set label. This process could result in bypassing of the security access control system.

C

Capability Maturity Model Integration (CMMI)—CMMI is a model used by many organizations to identify best practices useful in helping them assess and increase the maturity of their software development processes.

Capacity stress testing—Testing an application with large quantities of data to evaluate its performance during peak periods. Also called volume testing.

Card swipe—A physical control technique that uses a secured card or ID to gain access to a highly sensitive location. If built correctly, card swipes act as a preventive control over physical access to those sensitive locations. After a card

has been swiped, the application attached to the physical card swipe device logs all card users who try to access the secured location. The card swipe device prevents unauthorized access and logs all attempts to enter the secured location.

Central processing unit (CPU)—Computer hardware that houses the electronic circuits that control/direct all operations of the computer system

Certificate (certification) authority (CA)—A trusted third party that serves authentication infrastructures or organizations, and registers entities and issues them certificates

Certificate revocation list (CRL)—An instrument for checking the continued validity of the certificates for which the certification authority (CA) has responsibility. The CRL details digital certificates that are no longer valid. The time gap between two updates is very critical and is also a risk in digital certificates verification.

Certification practice statement (CPS)—A detailed set of rules governing the certificate authority's operations. It provides an understanding of the value and trustworthiness of certificates issued by a given CA. In terms of the controls that an organization observes, the method it uses to validate the authenticity of certificate applicants and the CA's expectations of how its certificates may be used.

Chain of custody—A legal principle regarding the validity and integrity of evidence. It requires accountability for anything that will be used as evidence in a legal proceeding to ensure that it can be accounted for from the time it was collected until the time it is presented in a court of law. Includes documentation as to who had access to the evidence and when, as well as the ability to identify evidence as being the exact item that was recovered or tested. Lack of control over evidence can lead to it being discredited. Chain of custody depends on the ability to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence, so it cannot be changed, and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering.

Challenge/response token—A method of user authentication that is carried out through use of the Challenge Handshake Authentication Protocol (CHAP). When a user tries to log into the server using CHAP, the server sends the user a

“challenge,” which is a random value. The user enters a password, which is used as an encryption key to encrypt the “challenge” and return it to the server. The server is aware of the password. It, therefore, encrypts the “challenge” value and compares it with the value received from

the user. If the values match, the user is authenticated. The challenge/response activity continues throughout the session and this protects the session from password sniffing attacks. In addition, addition, CHAP is not vulnerable to “man-in-the-middle” attacks because the challenge value is a random value that changes on each access attempt.

Change management—A holistic and proactive approach to managing the transition from a current to a desired organizational state, focusing specifically on the critical human or “soft” elements of change. Includes activities such as culture change (values, beliefs and attitudes), development of reward systems (measures and appropriate incentives) incentives), organizational design, stakeholder management, human resources (HR) policies and procedures, executive coaching, change leadership training, team building and communication planning and execution

Channel Service Unit/Digital Service Unit (CSU/DSU)—Interfaces at the physical layer of the open systems interconnection (OSI) reference model, data terminal equipment (DTE) to data circuit terminating equipment (DCE), for switched carrier networks

Check digit—A numeric value, which has been calculated mathematically, that is added to data to ensure that original data have not been altered or that an incorrect, but valid match has occurred. Check digit control is effective in detecting transposition and transcription errors.

Checklist—A list of items that is used to verify the completeness of a task or goal. Used in quality assurance (and, in general, in information systems audit) to check process compliance, code standardization and error prevention, and other items for which consistency processes or standards have been defined.

Checkpoint restart procedures—A point in a routine at which sufficient information can be stored to permit restarting the computation from that point.

Checksum—A mathematical value that is assigned to a file and used to

“test” the file at a later date to verify that the data contained in the file have

not been maliciously changed. A cryptographic checksum is created by performing a complicated series of mathematical operations (known as a cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as the checksum. Without knowing which cryptographic algorithm was used to create the hash value, it is highly unlikely that an unauthorized person would be able to change data without inadvertently changing the corresponding checksum. Cryptographic checksums are used in data transmission and data storage. Cryptographic checksums are also known as message authentication codes, integrity check-values, modification detection codes or message integrity codes.

Ciphertext—Information generated by an encryption algorithm to protect the plaintext and that is unintelligible to the unauthorized reader.

Circuit-switched network—A data transmission service requiring the establishment of a circuit-switched connection before data can be transferred from source data terminal equipment (DTE) to a sink DTE. A circuit-switched data transmission service uses a connection network.

Circular routing—In open systems architecture, circular routing is the logical path of a message in a communication network based on a series of gates at the physical network layer in the open systems interconnection (OSI) model.

Client-server—A group of computers connected by a communications network, in which the client is the requesting machine and the server is the supplying machine. Software is specialized at both ends. Processing may take place on either the client or the server, but it is transparent to the user.

Cloud computing—A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction
Coaxial cable—Composed of an insulated wire that runs through the middle of each cable, a second wire that surrounds the insulation of the inner wire like a sheath, and the outer insulation which wraps the second wire. Has a

greater transmission capacity than standard twisted-pair cables but has a limited range of effective distance.

Cohesion—The extent to which a system unit—subroutine, program, module, component, subsystem—performs a single dedicated function.

Generally, the more cohesive are units, the easier it is to maintain and enhance a system because it is easier to determine where and how to apply a change.

Cold site—An IS backup facility that has the necessary electrical and physical components of a computer facility but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event the users have to move from their main computing location to the alternative computer facility.

Communication processor—A computer embedded in a communications system that generally performs basic tasks of classifying network traffic and enforcing network policy functions. An example is the message data processor of a digital divide network (DDN) switching center. More advanced communications processors may perform additional functions.

Comparison program—A program for the examination of data, using logical or conditional tests to determine or to identify similarities or differences

Compensating control—An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions **Compiler**—A program that translates programming language (source code) into machine executable instructions (object code)

Completely connected (mesh) configuration—A network topology in which devices are connected with many redundant interconnections between network nodes (primarily used for backbone networks)

Completeness check—A procedure designed to ensure that no fields are missing from a record

Compliance testing—Tests of control designed to obtain audit evidence on both the effectiveness of the controls and their operation during the audit period

Components (as in component-based development)—Cooperating packages of executable software that make their services available through defined interfaces. Components used in developing systems may be commercial off-the-shelf software (COTS) or may be purposely built.

However, the goal of component-based development is to ultimately use as many predeveloped, pretested components as possible.

Comprehensive audit—An audit designed to determine the accuracy of financial records as well as evaluate the internal controls of a function or department

Computer emergency response team (CERT)—A group of people integrated at the organization with clear lines of reporting and responsibilities for standby support in case of an information systems emergency. This group acts as an efficient corrective control and should also act as a single point of contact for all incidents and issues related to information systems.

Computer forensics—The application of the scientific method to digital media to establish factual information for judicial review. This process often involves investigating computer systems to determine whether they are or have been used for illegal or unauthorized activities. As a discipline, it combines elements of law and computer science to collect and analyze data from information systems (e.g., personal computers, networks, wireless communications and digital storage devices) in a way that is admissible as evidence in a court of law.

Computer sequence checking—Verifies that the control number follows sequentially and that any control numbers out of sequence are rejected or noted on an exception report for further research

Computer-aided software engineering (CASE)—The use of software packages that aid in the development of all phases of an information system.

System analysis, design programming and documentation are provided.

Changes introduced in one CASE chart will update all other related charts automatically. CASE can be installed on a microcomputer for easy access.

Computer-assisted audit technique (CAAT)—Any automated audit technique, such as generalized audit software (GAS), test data generators, computerized audit programs and specialized audit utilities

Concurrency control—Refers to a class of controls used in database management systems (DBMS) to ensure that transactions are processed in an atomic, consistent, isolated and durable manner (ACID). This implies that only

serial and recoverable schedules are permitted, and that committed transactions are not discarded when undoing aborted transactions.

Configuration management—The control of changes to a set of configuration items over a system life cycle

Console log—An automated detail report of computer system activity
Contingency planning—Process of developing advance arrangements and procedures that enable an enterprise to respond to an event that could occur by chance or unforeseen circumstances

Continuity—Preventing, mitigating and recovering from disruption. The terms "business resumption planning," "disaster recovery planning" and

"contingency planning" also may be used in this context; they all concentrate on the recovery aspects of continuity.

Continuous auditing approach—This approach allows IS auditors to monitor system reliability on a continuous basis and to gather selective audit evidence through the computer.

Continuous improvement—The goals of continuous improvement (Kaizen) include the elimination of waste, defined as "activities that add cost, but do not add value;" just-in-time (JIT) delivery; production load leveling of amounts and types; standardized work; paced moving lines; right-sized equipment. A closer definition of the Japanese usage of Kaizen is "to take it apart and put back together in a better way." What is taken apart is usually a

process, system, product or service. Kaizen is a daily activity whose purpose goes beyond improvement. It is also a process that, when done correctly, humanizes the workplace, eliminates hard work (both mental and physical), and teaches people how to do rapid experiments using the scientific method and how to learn to see and eliminate waste in business processes.

Control group—Members of the operations area that are responsible for the collection, logging and submission of input for the various user groups **Control objective**—A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process **Control practice**—Key control mechanism that supports the achievement of control objectives through responsible use of resources, appropriate management of risk and alignment of

IT with business

Control risk—The risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls **Control section**—The area of the central processing unit (CPU) that executes software, allocates internal memory and transfers operations between the arithmetic-logic, internal storage and output sections of the computer **Cookie**—A message kept in the web browser for the purpose of identifying users and possibly preparing customized web pages for them. The first time a cookie is set, a user may be required to go through a registration process.

Subsequent to this, whenever the cookie's message is sent to the server, a customized view based on that user's preferences can be produced. The browser's implementation of cookies has, however, brought several security concerns, allowing breaches of security and the theft of personal information (e.g., user passwords that validate the user's identity and enable restricted web services).

Corporate governance—The system by which organizations are directed and controlled. The board of directors are responsible for the governance of their organizations. It consists of the leadership and organizational structures and processes that ensure the organization sustains and extends strategies and

objectives.

Corrective control—Designed to correct errors, omissions and unauthorized uses and intrusions once they are detected

Countermeasure—Any process that directly reduces a threat or vulnerability **Coupling**—Measure of interconnectivity among structure of software programs. Coupling depends on the interface complexity between modules.

This can be defined as the point at which entry or reference is made to a module, and what data pass across the interface. In application software design, it is preferable to strive for the lowest possible coupling between modules. Simple connectivity among modules results in software that is easier to understand and maintain, and less prone to a ripple or domino effect caused when errors occur at one location and propagate through a system.

Critical infrastructure—Systems whose incapacity or destruction would have a

debilitating effect on the economic security of an enterprise, community or nation

Critical success factor (CSF)—The most important issue or action for management to achieve control over and within its IT processes

Customer relationship management (CRM)—A way to identify, acquire and retain customers. CRM is also an industry term for software solutions that help an organization manage customer relationships in an organized manner.

D

Data communications—The transfer of data between separate computer processing sites/devices using telephone lines, microwave and/or satellite links

Data custodian—Individual(s) and department(s) responsible for the storage and safeguarding of computerized information. This typically is within the IS

organization.

Data dictionary—A database that contains the name, type, range of values, source, and authorization for access for each data element in a database. It also indicates which application programs use those data so that when a data structure is contemplated, a list of the affected programs can be generated.

May be a stand-alone information system used for management or

documentation purposes, or it may control the operation of a database.

Data diddling—Changing data with malicious intent before or during input into the system

Data Encryption Standard (DES)—An algorithm for encoding binary data.

It is a secret key cryptosystem published by the National Bureau of Standards (NBS), the predecessor of the US National Institute of Standards and Technology (NIST). DES was defined as a Federal Information Processing Standard (FIPS) in 1976 and has been used commonly for data encryption in the forms of software and hardware implementation. (See private key cryptosystem.)

Data leakage—Siphoning out or leaking information by dumping computer files or stealing computer reports and tapes

Data owner—Individual(s), normally a manager or director, who have responsibility for the integrity, accurate reporting and use of computerized data

Data security—Those controls that seek to maintain confidentiality, integrity and availability of information

Data structure—The relationships among files in a database and among data items within each file

Database—A stored collection of related data needed by organizations and individuals to meet their information processing and retrieval requirements
Database administrator (DBA)—An individual or department responsible for the security and information classification of the shared data stored on a database system. This responsibility includes the design, definition and

maintenance of the database.

Database management system (DBMS)—A software system that controls the organization, storage and retrieval of data in a database

Database replication—The process of creating and managing duplicate versions of a database. Replication not only copies a database but also synchronizes a set of replicas so that changes made to one replica are reflected in all of the others. The beauty of replication is that it enables many users to work with their own local copy of a database, but have the database updated as if they were working on a single centralized database. For database applications in which, geographically users are distributed widely, replication is often the most efficient method of database access.

Database specifications—These are the requirements for establishing a database application. They include field definitions, field requirements, and reporting requirements for the individual information in the database.

Data-oriented systems development—Focuses on providing ad hoc reporting for users by developing a suitable accessible database of information and to provide useable data rather than a function

Decentralization—The process of distributing computer processing to different locations within an organization

Decision support system (DSS)—An interactive system that provides the user with easy access to decision models and data, to support semistructured decision-making tasks

Decryption—A technique used to recover the original plaintext from the ciphertext such that it is intelligible to the reader. The decryption is a reverse process of the encryption.

Decryption key—A piece of information used to recover the plaintext from the corresponding ciphertext by decryption

Degauss—The application of variable levels of alternating current for the

purpose of demagnetizing magnetic recording media. The process involves increasing the alternating current field gradually from zero to some maximum value and back to zero, leaving a very low residue of magnetic induction on the media. Degauss loosely means to erase.

Demodulation—The process of converting an analog telecommunications signal into a digital computer signal.

Detection risk—The risk that material errors or misstatements that have occurred will not be detected by the IS auditor

Detective control—Exists to detect and report when errors, omissions and unauthorized uses or entries occur.

Dial-back—Used as a control over dial-up telecommunications lines. The telecommunications link established through dial-up into the computer from a remote location is interrupted so the computer can dial back to the caller. The link is permitted only if the caller is from a valid phone number or telecommunications channel.

Dial-in access control—Prevents unauthorized access from remote users who attempt to access a secured environment. Ranges from a dial-back control to remote user authentication.

Digital certificate—A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and nonrepudiation. A digital signature is generated using the sender's private key or applying a one-way hash function.

Digital signature—A piece of information, a digitized form of a signature, that provides sender authenticity, message integrity and nonrepudiation. A digital signature is generated using the sender's private key or applying a one-way hash function.

Disaster recovery plan (DRP)—A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster

Disaster tolerance—The time gap during which the business can accept the non-availability of IT facilities.

Discovery sampling—A form of attribute sampling that is used to determine a specified probability of finding at least one example of an occurrence (attribute) in a population

Discretionary access control (DAC)—A means of restricting access to objects based on the identity of subjects and/or groups to which they belong.

The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Diskless workstations—A workstation or PC on a network that does not have its own disk, but instead stores files on a network file server **Distributed data processing network**—A system of computers connected together by a communications network. Each computer processes its data and the network supports the system as a whole. Such a network enhances communication among the linked computers and allows access to shared files.

Diverse routing—The method of routing traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities

by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. However, acquiring this type of access is time-consuming and costly. Most carriers provide facilities for alternate and diverse routing, although the majority of services are transmitted over terrestrial media. These cable facilities are usually located in the ground or basement. Ground-based facilities are at great risk due to the aging infrastructures of cities. In addition, cable-based facilities usually share room with mechanical and electrical

systems that can impose great risk due to human error and disastrous events.

Domain name system (DNS)—A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services, such as web and email servers

Domain name system (DNS) poisoning—Corrupts the table of an Internet server's DNS, replacing an Internet address with the address of another vagrant or scoundrel address. If a web user looks for the page with that address, the request is redirected by the scoundrel entry in the table to a different address. Cache poisoning differs from another form of DNS

poisoning in which the attacker spoofs valid email accounts and floods the

"n" boxes of administrative and technical contacts. Cache poisoning is related to URL poisoning or location poisoning, in which an Internet user behavior is tracked by adding an identification number to the location line of the browser that can be recorded as the user visits successive pages on the site. It is also called DNS cache poisoning or cache poisoning.

Downloading—The act of transferring computerized information from one computer to another computer

Downtime report—A report that identifies the elapsed time when a computer is not operating correctly because of machine failure

Dry-pipe fire extinguisher system—Refers to a sprinkler system that does not have water in the pipes during idle usage, unlike a fully charged fire extinguisher system that has water in the pipes at all times. The dry-pipe system is activated at the time of the fire alarm and water is emitted to the pipes from a water

reservoir for discharge to the location of the fire.

Dumb terminal—A display terminal without processing capability. Dumb terminals are dependent on the main computer for processing. All entered data are accepted without further editing or validation.

Dynamic Host Configuration Protocol (DHCP)—A protocol used by networked computers (clients) to obtain IP addresses and other parameters, such as the default gateway, subnet mask and IP addresses of domain name

system (DNS) servers from a DHCP server. The DHCP server ensures that all IP addresses are unique (e.g., no IP address is assigned to a second client while the first client's assignment is valid [its lease has not expired]). Thus, IP address pool management is done by the server and not by a human network administrator.

E

Echo checks—Detects line errors by retransmitting data back to the sending device for comparison with the original transmission

Ecommerce—The processes by which enterprises conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology. Ecommerce encompasses both business-to-business (B2B) and business-to-consumer (B2C) ecommerce models but does not include existing non-Internet Internet ecommerce methods based on private networks, such as electronic data interchange (EDI) and Society for Worldwide Interbank Financial

Telecommunication (SWIFT).

Edit control—Detects errors in the input portion of information that is sent to the computer for processing. May be manual or automated and allow the user to edit data errors before processing.

Editing—Ensures that data conform to predetermined criteria and enable early identification of potential errors

Electronic data interchange (EDI)—The electronic transmission of transactions (information) between two organizations. EDI promotes a more

efficient paperless environment. EDI transmissions can replace the use of standard documents, including invoices or purchase orders.

Electronic funds transfer (EFT)—The exchange of money via telecommunications. EFT refers to any financial transaction that originates at a terminal and transfers a sum of money from one account to another.

Email/interpersonal messaging—An individual using a terminal, PC or an

application can access a network to send an unstructured message to another individual or group of people

Embedded audit module (EAM)—Integral part of an application system that is designed to identify and report specific transactions or other information based on predetermined criteria. Identification of reportable items occurs as part of real-time processing. Reporting may be real-time online or may use store and forward methods. Also known as integrated test facility or continuous auditing module.

Encapsulation (objects)—The technique used by layered protocols in which a lower-layer protocol accepts a message from a higher-layer protocol and places it in the data portion of a frame in the lower layer.

Encryption—The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext)

Encryption key—A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext to the ciphertext

End-user computing—The ability of end users to design and implement their own information system utilizing computer software products **Enterprise resource planning (ERP)**—A packaged business software system that allows an organization to automate and integrate the majority of its business processes, share common data and practices across the entire organization, and produce and access information in a real-time environment.

Examples of ERP include SAP, Oracle Financials and J.D. Edwards.

Escrow agent—A person, agency or organization that is authorized to act on

behalf of another to create a legal relationship with a third party in regard to an escrow agreement; the custodian of an asset according to an escrow agreement. As it relates to a cryptographic key, an escrow agent is the agency or organization charged with the responsibility for safeguarding the key components of the unique key.

Escrow agreement—A legal arrangement whereby an asset (often money, but sometimes other property, such as art, a deed of title, website, software source code or a cryptographic key) is delivered to a third party (called an escrow agent) to be held in trust or otherwise pending a contingency or the fulfillment of a condition or conditions in a contract. Upon the occurrence of the escrow agreement, the escrow agent will deliver the asset to the proper recipient; otherwise the escrow agent is bound by his/her fiduciary duty to maintain the escrow account. Source code escrow means deposit of the source code for the software into an account held by an escrow agent. Escrow is typically requested by a party licensing software (e.g., licensee or buyer) to ensure maintenance of the software. The software source code is released by the escrow agent to the licensee if the licensor (e.g., seller or contractor) files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement.

Ethernet—A popular network protocol and cabling scheme that uses a bus topology and carrier sense multiple access/collision detection (CSMA/CD) to prevent network failures or collisions when two devices try to access the network at the same time

Evidence—The information an auditor gathers in the course of performing an IS audit; relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support **Exception reports**—An exception report is generated by a program that identifies transactions or data that appear to be incorrect. Exception reports may be outside a predetermined range or may not conform to specified criteria.

Exclusive-OR (XOR)—The exclusive-OR operator returns a value of TRUE

only if just one of its operands is TRUE. The XOR operation is a Boolean operation that produces a 0 if its two Boolean inputs are the same (0 and 0 or 1 and 1) and it produces a 1 if its two inputs are different (1 and 0). In contrast, an inclusive-OR operator returns a value of TRUE if either or both of its operands

are TRUE.

Executable code—The machine language code that is generally referred to as the object or load module

Expert system—The most prevalent type of computer system that arises from the research of artificial intelligence. An expert system has a built-in hierarchy of rules, which are acquired from human experts in the appropriate field. Once input is provided, the system should be able to define the nature of the problem and provide recommendations to solve the problem.

Exposure—The potential loss to an area due to the occurrence of an adverse event

Extended Binary-coded Decimal Interchange Code (EBCDIC)—An 8-bit code representing 256 characters; used in most large computer systems
Extensible Markup Language (XML)—Promulgated through the World Wide Web Consortium, XML is a web-based application development

technique that allows designers to create their own customized tags, thus enabling the definition, transmission, validation and interpretation of data between applications and organizations

Extranet—A private network that resides on the Internet and allows a company to securely share business information with customers, suppliers, or other businesses as well as to execute electronic transactions. different from an intranet in that it is located beyond the company's firewall. Therefore, an extranet relies on the use of securely issued digital certificates (or alternative methods of user authentication) and encryption of messages. A virtual private network (VPN) and tunneling are often used to implement extranets, to ensure security and privacy.

F

Fallback procedures—A plan of action or set of procedures to be performed if a system implementation, upgrade or modification does not work as intended. May involve restoring the system to its state prior to the implementation or change. Fallback procedures are needed to ensure that normal business processes continue in the event of failure and should always

be considered in system migration or implementation.

False authorization—Also called false acceptance; occurs when an unauthorized person is identified as an authorized person by the biometric system.

False enrollment—Occurs when an unauthorized person manages to enroll into the biometric system. Enrollment is the initial process of acquiring a biometric feature and saving it as a personal reference on a smart card, a PC

or in a central database.

Fault tolerance—A system's level of resilience to seamlessly react to hardware and/or software failure

Feasibility study—A phase of a system development life cycle (SDLC) methodology that researches the feasibility and adequacy of resources for the development or acquisition of a system solution to a user need

Fiber-optic cable—Glass fibers that transmit binary signals over a telecommunications network. Fiber-optic systems have low transmission losses as compared to twisted-pair cables. They do not radiate energy or conduct electricity. They are free from corruption and lightning-induced interference, and they reduce the risk of wiretaps.

Field—An individual data element in a computer record. Examples include employee name, customer address, account number, product unit price and product quantity in stock.

File—A named collection of related records

File allocation table (FAT)—A table used by the operating system to keep track of where every file is located on the disk. Since a file is often fragmented, and thus subdivided into many sectors within the disk, the information stored in the FAT is used when loading or updating the contents of the file.

File layout—Specifies the length of the file's record, and the sequence and

size of its fields. Also will specify the type of data contained within each field: for example, alphanumeric, zoned decimal, packed and binary.

File server—A high-capacity disk storage device or a computer that stores data centrally for network users and manages access to that data. File servers can be dedicated so that no process other than network management can be executed while the network is available; file servers can be nondedicated so that standard user applications can run while the network is available.

File Transfer Protocol (FTP)—A protocol used to transfer files over a Transmission Control Protocol/Internet Protocol (TCP/IP) network (Internet, UNIX, etc.)

Financial audit—An audit designed to determine the accuracy of financial records and information

Firewall—A system or combination of systems that enforces a boundary between two or more networks typically forming a barrier between a secure and an open environment, such as the Internet

Firmware—Memory chips with embedded program code that hold their content when power is turned off

Foreign key—A value that represents a reference to a tuple (a row in a table) containing the matching candidate key value. The problem of ensuring that the database does not include any invalid foreign key values is known as the referential integrity problem. The constraint that values of a given foreign key must match values of the corresponding candidate key is known as a referential constraint. The relation (table) that contains the foreign key is referred to as the referencing relation and the relation that contains the corresponding candidate key as the referenced relation or target relation. (In the relational theory it would be a candidate key, but in real database management systems (DBMSs) implementations it is always the primary key.)

Format checking—The application of an edit, using a predefined field definition to a submitted information stream; a test to ensure that data

conform to a predefined format

Fourth-generation language (4GL)—High-level, user-friendly, nonprocedural computer languages used to program and/or read and process computer files

Frame relay—A packet-switched wide-area network (WAN) technology that

provides faster performance than older packet-switched WAN technologies.

Best suited for data and image transfers. Because of its variable-length packet architecture, it is not the most efficient technology for real-time voice and video. In a frame-relay network, end nodes establish a connection via a permanent virtual circuit (PVC).

Function point analysis—A technique used to determine the size of a development task, based on the number of function points. Function points are factors, such as inputs, outputs, inquiries and logical internal sites.

G

Gateway—A device (router, firewall) on a network that serves as an entrance to another network

General computer control—A control, other than an application control, that relates to the environment within which computer-based application systems are developed, maintained and operated, and that is therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications and the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS

strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.

Generalized audit software (GAS)—Multipurpose audit software that can be used for general processes, such as record selection, matching, recalculation and reporting

Geographical information system (GIS)—A tool used to integrate, convert, handle, analyze and produce information regarding the surface of the earth.

GIS data exist as maps, tridimensional virtual models, lists and tables.

Governance—Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring

performance and compliance against agreed-on direction and objectives. Conditions can include the cost of capital, foreign exchange rates, etc. Options can include shifting manufacturing to other locations, subcontracting portions of the enterprise to third parties, selecting a product mix from many available choices, etc.

H

Hacker—An individual who attempts to gain unauthorized access to a computer system

Handprint scanner—A biometric device that is used to authenticate a user through palm scans

Hardware—The physical components of a computer system

Hash total—The total of any numeric data field in a document or computer file. This total is checked against a control total of the same field to facilitate accuracy of processing.

Help desk—A service offered via phone/Internet by an organization to its clients or employees that provides information, assistance, and

troubleshooting advice regarding software, hardware, or networks. A help desk is staffed by people that can either resolve the problem on their own or escalate the problem to specialized personnel. A help desk is often equipped with dedicated customer relationship management (CRM) software that logs the problems and tracks them until they are solved.

Heuristic filter—A method often employed by antispam software to filter spam using criteria established in a centralized rule database. Every email

message is given a rank, based upon its header and contents, which is then matched against preset thresholds. A message that surpasses the threshold will be flagged as spam and discarded, returned to its sender or put in a spam directory for further review by the intended recipient.

Hexadecimal—A numbering system that uses a base of 16 and uses 16

digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F. Programmers use

hexadecimal numbers as a convenient way of representing binary numbers.

Hierarchical database—A database structured in a tree/root or parent/child relationship. Each parent can have many children, but each child may have only one parent.

Honeypot—A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems.

Hot site—A fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of a disaster **Hypertext Markup Language (HTML)**—A language designed for the creation of web pages with hypertext and other information to be displayed in a web browser. HTML is used to structure information—denoting certain text as headings, paragraphs, lists and so on—and can be used to describe, to some degree, the appearance and semantics of a document.

I

Image processing—The process of electronically inputting source documents by taking an image of the document, thereby eliminating the need for key entry

Impact assessment—A review of the possible consequences of a risk **Impersonation**—A security concept related to Windows NT that allows a server application to temporarily "be" the client in terms of access to secure objects. Impersonation has three possible levels: identification, letting the

server inspect the client's identity; impersonation, letting the server act on behalf of the client; and delegation, the same as impersonation but extended to remote systems to which the server connects (through the preservation of credentials). Impersonation by imitating or copying the identification, behavior or actions of another may also be used in social engineering to obtain otherwise unauthorized physical access.

Incident—Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service.

Incident response—The response of an enterprise to a disaster or other

significant event that may significantly affect the enterprise, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan (DRP), performing damage assessment, and any other measures necessary to bring an enterprise to a more stable status.

Incremental testing—Deliberately testing only the value-added functionality of a software component

Independence—An IS auditor's self-governance and freedom from conflict of interest and undue influence. The IS auditor should be free to make his/her own decisions, not influenced by the organization being audited and its people (managers and employees).

Indexed sequential access method (ISAM)—A disk access method that stores data sequentially while also maintaining an index of key fields to all the records in the file for direct access capability

Information processing facility (IPF)—The computer room and support areas

Information security—Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability)

Information security governance—The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly

Information systems (IS)—The combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies. Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components.

Inherent risk—The risk level or exposure without considering the actions that management has taken or might take (e.g., implementing controls) **Inheritance (objects)**—Database structures that have a strict hierarchy (no multiple inheritance). Inheritance can initiate other objects irrespective of the class

hierarchy, thus there is no strict hierarchy of objects

Initial program load (IPL)—The initialization procedure that causes an operating system to be loaded into storage at the beginning of a workday or after a system malfunction

Input control—Techniques and procedures used to verify, validate and edit data, to ensure that only correct data are entered into the computer **Instant messaging (IM)**—An online mechanism or a form of real-time communication among two or more people based on typed text and

multimedia data. The text is conveyed via computers or another electronic device (e.g., cell phone or handheld device) connected over a network, such as the Internet.

Integrated services digital network (ISDN)—A public end-to-end, digital telecommunications network with signaling, switching, and transport capabilities supporting a wide range of service accessed by standardized interfaces with integrated customer control. The standard allows transmission of digital voice, video and data over 64 kbps lines.

Integrated test facilities (ITF)—A testing methodology where test data are processed in production systems. The data usually represent a set of fictitious entities, such as departments, customers and products. Output reports are verified to confirm the correctness of the processing.

Integrity—The guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity

Interface testing—A testing technique that is used to evaluate output from one application while the information is sent as input to another application **Internal controls**—The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved, and undesired events will be prevented or detected and corrected

Internet—1) Two or more networks connected by a router; 2) the world's largest network using Transmission Control Protocol/Internet Protocol (TCP/IP) to link government, university and commercial institutions.

Internet Engineering Task Force (IETF)—An organization with international

affiliates as network industry representatives that sets Internet standards. This includes all network industry developers and researchers concerned with the evolution and planned growth of the Internet.

Internet packet (IP) spoofing—An attack using packets with the spoofed source Internet packet (IP) addresses. This technique exploits applications that use authentication based on IP addresses. This technique also may enable an unauthorized user to gain root access on the target system.

Internet Protocol Security (IPSec)—A set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets

Irregularity—Intentional violations of established management policy or regulatory requirement. It may consist of deliberate misstatements or

omissions of information concerning the area under audit or the organization as a whole; gross negligence or unintentional illegal acts.

Internet Security Association and Key Management Protocol (ISAKMP)

—A protocol for sharing a public key

IT governance framework—A model that integrates a set of guidelines, policies and methods that represent the organizational approach to the IT

governance. Per COBIT, IT governance is the responsibility of the board of directors and executive management. It is an integral part of institutional governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives.

IT incident—Any event that is not part of the ordinary operation of a service that causes, or may cause, an interruption to, or a reduction in, the quality of that service

IT infrastructure—The set of hardware, software and facilities that integrates an organization's IT assets. Specifically, the equipment (including servers, routers, switches, and cabling), software, services and products used in storing, processing, transmitting and displaying all forms of information for the

organization’s users.

IT steering committee—An executive-management-level committee that assists in the delivery of the IT strategy, oversees day-to-day management of IT service delivery and IT projects, and focuses on implementation aspects **IT strategic plan**—A long-term plan (i.e., three- to five-year horizon) in which business and IT management cooperatively describe how IT resources will contribute to the enterprise’s strategic objectives (goals) **IT strategy committee**—A committee at the level of the board of directors to ensure that the board is involved in major IT matters and decisions. The committee is primarily accountable for managing the portfolios of IT-enabled investments, IT services and other IT resources. The committee is the owner of the portfolio.

J

Judgment sampling—Any sample that is selected subjectively or in such a manner that the sample selection process is not random or the sampling results are not evaluated mathematically

K

Key goal indicator (KGI)—A measure that tells management, after the fact, whether an IT process has achieved its business requirements; usually expressed in terms of information criteria

Key management practice—Management practices that are required to successfully execute business processes

Key performance indicator (KPI)—A measure that determines how well the process is performing in enabling the goal to be reached. A lead indicator of whether a goal will likely be reached or not, and a good indicator of capabilities, practices and skills. It measures the activity goal, which is an action that the process owner must take to achieve effective process performance.

L

Leased line—A communication line permanently assigned to connect two points, as opposed to a dial up line that is only available and open when a connection is made by dialing the target machine or network. Also known as a dedicated line.

Librarian—The individual responsible for the safeguard and maintenance of all program and data files

Licensing agreement—A contract that establishes the terms and conditions under which a piece of software is being licensed (i.e., made legally available for use) from the software developer (owner) to the user

Life cycle—A series of stages that characterize the course of existence of an organizational investment (e.g., product, project, program)

Limit check—Tests specified amount fields against stipulated high or low limits of acceptability. When both high and low values are used, the test may be called a range check.

Literals—Any notation for representing a value within programming language source code (e.g., a string literal); a chunk of input data that is represented "as is" in compressed data

Local area network (LAN)—Communication network that serves several users within a specified geographical area. A personal computer LAN

functions as distributed processing system in which each computer in the network does its own processing and manages some of its data. Shared data are stored in a file server that acts as a remote disk drive for all users in the network.

Log—To record details of the information or events in an organized record-keeping system, usually sequenced in the order in which they occurred **Logical access controls**—The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data files

Logon—The act of connecting to the computer, which typically requires entry of a user ID and password into a computer terminal

M

Magnetic card reader—Reads cards with a magnetic surface on which data can be stored and retrieved

Malware—Short for malicious software. Designed to infiltrate, damage or

obtain information from a computer system without the owner’s consent.

Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, is not really malicious although it is generally unwanted. Spyware can, however, be used to gather information for identity theft or other clearly illicit purposes.

Management information system (MIS)—An organized assembly of resources and procedures required to collect, process and distribute data for use in decision making

Mandatory access controls (MAC)—A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users or programs acting on their behalf

Mapping—Diagramming data that is to be exchanged electronically, including how they are to be used and what business management systems need them. Mapping is a preliminary step for developing an applications link.

(See application tracing and mapping.)

Masking—A computerized technique of blocking out the display of sensitive information, such as passwords, on a computer terminal or report **Master file**—A file of semi-permanent information that is used frequently for processing data or for more than one purpose

Materiality—An auditing concept regarding the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited. An expression of the relative significance or importance of a particular matter in the context of the organization as a whole.

Maturity—In business, indicates the degree of reliability or dependency that the business can place on a process achieving the desired goals or objectives **Maturity model**—See capability maturity model (CMM).

Media Access Control (MAC)—Applied to the hardware at the factory and cannot be modified, MAC is a unique, 48-bit, hard-coded address of a physical layer device, such as an Ethernet local area network (LAN) or a wireless network card.

Media oxidation—The deterioration of the media on which data are digitally stored due to exposure to oxygen and moisture. Tapes deteriorating in a

warm, humid environment are an example of media oxidation. Proper environmental controls should prevent, or significantly slow, this process.

Memory dump—The act of copying raw data from one place to another with little or no formatting for readability. Usually, dump refers to copying data from the main memory to a display screen or a printer. Dumps are useful for diagnosing bugs. After a program fails, one can study the dump and analyze the contents of memory at the time of the failure. A memory dump will not help unless each person knows what to look for because dumps are usually output in a difficult-to-read form (binary, octal or hexadecimal).

Message switching—A telecommunications methodology that controls traffic in which a complete message is sent to a concentration point and stored until the communications path is established

Microwave transmission—A high-capacity line-of-sight transmission of data signals through the atmosphere which often requires relay stations **Middleware**—Another term for an application programmer interface (API).

It refers to the interfaces that allow programmers to access lower- or higher-level services by providing an intermediary layer that includes function calls to the services.

Milestone—A terminal element that marks the completion of a work package or phase. Typically marked by a high-level event, such as project completion, receipt, endorsement or signing of a previously-defined deliverable or a high-level review meeting at which the appropriate level of project completion is

determined and agreed to. A milestone is associated with some sort of decision that outlines the future of a project and, for an outsourced project, may have a payment to the contractor associated with it.

Mission-critical application—An application that is vital to the operation of the organization. The term is very popular for describing the applications required to run the day-to-day business.

Mobile site—The use of a mobile/temporary facility to serve as a business resumption location. The facility can usually be delivered to any site and can

house information technology and staff.

Modulation—The process of converting a digital computer signal into an analog telecommunications signal

Monetary unit sampling—A sampling technique that estimates the amount of overstatement in an account balance

N

Network—A system of interconnected computers and the communications equipment used to connect them

Network administrator—Responsible for planning, implementing and maintaining the telecommunications infrastructure; also may be responsible for voice networks. For smaller organizations, the network administrator may also maintain a local area network (LAN) and assist end users.

Network attached storage (NAS)—Utilize dedicated storage devices that centralize storage of data. NAS devices generally do not provide traditional file/print or application services.

Network interface card (NIC)—A communication card that when inserted into a computer, allows it to communicate with other computers on a network. Most NICs are designed for a particular type of network or protocol.

Noise—Disturbances in data transmissions, such as static, that cause messages to be misinterpreted by the receiver

Nondisclosure agreement (NDA)—A legal contract between at least two parties that outlines confidential materials the parties wish to share with one another for certain purposes but wish to restrict from generalized use; a contract through which the parties agree not to disclose information covered by the agreement. Also called a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement. An NDA creates a confidential relationship between the parties to protect any type of trade secret. As such, an NDA can protect non-public business information. In the

case of certain governmental entities, the confidentiality of information other than trade secrets may be subject to applicable statutory requirements and, in some cases, may be required to be revealed to an outside party requesting the information. Generally, the governmental entity will include a provision in the contract to allow the seller to review a request for information the seller identifies as confidential and the seller may appeal such a decision requiring disclosure. NDAs are commonly signed when two companies or individuals are considering doing business together and need to understand the processes used in one another's businesses solely for the purpose of evaluating the potential business relationship. NDAs can be "mutual," meaning both parties are restricted in their use of the materials provided, or they can only restrict a single party. It is also possible for an employee to sign an NDA or NDA-like agreement with a company at the time of hiring; in fact, some employment agreements will include a clause restricting "confidential information" in general.

Normalization—The elimination of redundant data

Numeric check—An edit check designed to ensure that the data element in a particular field is numeric

O

Object code—Machine-readable instructions produced from a compiler or assembler program that has accepted and translated the source code **Object orientation**—An approach to system development in which the basic unit of attention is an object, which represents an encapsulation of both data (an object's attributes) and functionality (an object's methods). Objects usually are created using a general template called a class. A class is the basis for most design work in objects. A class and its objects communicate in defined ways. Aggregate classes interact through messages, which are directed requests for services from

one class (the client) to another class (the server). A class may share the structure or methods defined in one or more other classes—a relationship known as inheritance.

Objectivity—The ability of the IS auditor to exercise judgment, express

opinions and present recommendations with impartiality **Offsite storage**—A facility located away from the building housing the primary information processing facility (IPF), used for storage of computer media, such as offline backup data and storage files

Online data processing—Achieved by entering information into the computer via a video display terminal. With online data processing, the computer immediately accepts or rejects the information as it is entered.

Open system—System for which detailed specifications of the composition of its component are published in a nonproprietary environment, thereby enabling competing enterprises to use these standard components to build competitive systems. The advantages of using open systems include portability, interoperability and integration.

Operating system (OS)—A master control program that runs the computer and acts as a scheduler and traffic controller. The operating system is the first program copied into the computer's memory after the computer is turned on; it must reside in memory at all times. It is the software that interfaces between the computer hardware (disk, keyboard, mouse, network, modem, printer) and the application software (word processor, spreadsheet, email), which also controls access to the devices and is partially responsible for security components and sets the standards for the application programs that run in it.

Operational audit—An audit designed to evaluate the various internal controls, economy and efficiency of a function or department

Operational control—Deals with the everyday operation of a company or organization to ensure that all objectives are achieved.

Operator console—A special terminal used by computer operations personnel to control computer and systems operations functions. Operator console terminals typically provide a high level of computer access and should be properly secured.

Optical scanner—An input device that reads characters and images that are printed or painted on a paper form into the computer

Outsourcing—A formal agreement with a third party to perform IS or other business functions for an enterprise

P

Packet—Data unit that is routed from source to destination in a packet-switched network. A packet contains both routing information and data.

Transmission Control Protocol/Internet Protocol (TCP/IP) is such a packet-switched network.

Packet switching—The process of transmitting messages in convenient pieces that can be reassembled at the destination

Paper test—A walk-through of the steps of a regular test, but without actually performing the steps. Usually used in disaster recovery and contingency testing; team members review and become familiar with the plans and their specific roles and responsibilities.

Parallel testing—The process of feeding test data into two systems, the modified system and an alternative system (possibly the original system), and comparing results to demonstrate the consistency and inconsistency between two versions of the application

Parity check—A general hardware control that helps to detect data errors when data are read from memory or communicated from one computer to another. A 1-bit digit (either 0 or 1) is added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, the computer reports an error. The probability of a parity check detecting an error is 50 percent.

Partitioned file—A file format in which the file is divided into multiple sub files and a directory is established to locate each sub file

Passive assault—Intruders attempt to learn some characteristic of the data

being transmitted. With a passive assault, intruders may be able to read the

contents of the data, so the privacy of the data is violated. Alternatively, although the content of the data itself may remain secure, intruders may read and analyze the plaintext source and destination identifiers attached to a message for routing purposes, or they may examine the lengths and frequency of messages being transmitted.

Password—A protected, generally computer-encrypted string of characters that authenticate a computer user to the computer system

Patch management—An area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system in order to maintain up-to-date software and often to address security risk. Patch management tasks include the following: maintaining current knowledge of available patches; deciding what patches are appropriate for particular systems; ensuring that patches are installed properly; testing systems after installation; and documenting all associated procedures, such as specific configurations required. A number of products are available to automate patch management tasks. Patches are sometimes ineffective and can sometimes cause more problems than they fix. Patch management experts suggest that system administrators take simple steps to avoid problems, such as performing backups and testing patches on noncritical systems prior to installations. Patch management can be viewed as part of change management.

Payroll system—An electronic system for processing payroll information and the related electronic (e.g., electronic timekeeping and/or human resources system), human (e.g., payroll clerk), and external party (e.g., bank) interfaces. In a more limited sense, it is the electronic system that performs the processing for generating payroll checks and/or bank direct deposits to employees.

Penetration testing—A live test of the effectiveness of security defenses through mimicking the actions of real life attackers

Performance driver—A measure that is considered the “driver” of a lag

indicator. It can be measured before the outcome is clear and, therefore, is called a “lead indicator.” There is an assumed relationship between the two that suggests that improved performance in a leading indicator will drive better performance in the lagging indicator. They are also referred to as key performance indicators (KPIs) and are used to indicate whether goals are likely

to be met.

Performance testing—Comparing the system's performance to other equivalent systems, using well-defined benchmarks

Peripherals—Auxiliary computer hardware equipment used for input, output and data storage. Examples of peripherals include disk drives and printers.

Personal identification number (PIN)—A type of password (i.e., a secret number assigned to an individual) that, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual.

PINs have been adopted by financial institutions as the primary means of verifying customers in an electronic funds transfer (EFT) system.

Phishing—This is a type of electronic mail (email) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering. Phishing attacks may take the form of masquerading as a lottery organization advising the recipient or the user's bank of a large win; in either case, the intent is to obtain account and personal identification number (PIN) details. Alternative attacks may seek to obtain apparently innocuous business information which may be used in another form of active attack.

Phreakers—Those who crack security, most frequently phone and other communication networks

Plaintext—Digital information, such as cleartext, that is intelligible to the reader

Point-of-sale (POS) systems—Enable the capture of data at the time and place of transaction. POS terminals may include use of optical scanners for use with bar codes or magnetic card readers for use with credit cards. POS

systems may be online to a central computer or may use stand-alone terminals or microcomputers that hold the transactions until the end of a specified period when they are sent to the main computer for batch processing.

Point-to-point protocol (PPP)—A protocol used for transmitting data between two ends of a connection

Policy—1. Generally, a document that records a high-level principle or course of action that has been decided on. The intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams. In addition to policy content, policies need to describe the consequences of failing to comply with the policy, the means for handling exceptions, and the manner in which compliance with the policy will be checked and measured.

2. Overall intention and direction as formally expressed by management (COBIT 5 perspective)

Portfolio—A grouping of "objects of interest" (investment programs, IT

services, IT projects, other IT assets or resources) managed and monitored to optimize business value (The investment portfolio is of primary interest to Val IT. IT service, project, asset and other resource portfolios are of primary interest to COBIT.)

Preventive control—An internal control that is used to avoid undesirable events, errors and other occurrences that an enterprise has determined could have a negative material effect on a process or end product

Privacy—The rights of an individual to trust that others will appropriately and respectfully use, store, share and dispose of his/her associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived. What is appropriate depends on the associated circumstances, laws and the individual's reasonable expectations.

An individual also has the right to reasonably control and be aware of the collection, use and disclosure of his\her associated personal and sensitive

information.

Private branch exchange (PBX)—A telephone exchange that is owned by a private business, as opposed to one owned by a common carrier or by a telephone company

Private key cryptosystem—Used in data encryption, it uses a secret key to encrypt the plaintext to the ciphertext. Private key cryptosystems also use the same key to decrypt the ciphertext to the corresponding plaintext. In this case,

the key is symmetric such that the encryption key is equivalent to the decryption key.

Problem escalation procedure—The process of escalating a problem up from junior to senior support staff, and ultimately to higher levels of management. Problem escalation procedure is often used in help desk management, when an unresolved problem is escalated up the chain of command, until it is solved.

Procedure—A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.

Process—Generally, a collection of activities influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs. Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance.

Production program—Program used to process live or actual data that were received as input into the production environment

Production software—Software that is being used and executed to support normal and authorized organizational operations. Production software is to be distinguished from test software, which is being developed or modified, but has not yet been authorized for use by management.

Professional competence—Proven level of ability, ability, often linked to qualifications issued by relevant professional bodies and compliance with their codes of practice and standards

Program Evaluation and Review Technique (PERT)—A project

management technique used in the planning and control of system projects
Program flowchart—Shows the sequence of instructions in a single program or subroutine. The symbols used in program flowcharts should be the internationally accepted standard. Program flowcharts should be updated when necessary.

Program narrative—Provides a detailed explanation of program flowcharts,

including control points and any external input

Project—A structured set of activities concerned with delivering a defined capability (that is necessary but not sufficient, to achieve a required business outcome) to the enterprise based on an agreed-on schedule and budget **Project portfolio**—The set of projects owned by a company. It usually includes the main guidelines relative to each project, including objectives, costs, time lines and other information specific to the project.

Protocol—The rules by which a network operates and controls the flow and priority of transmissions

Protocol converter—Hardware devices, such as asynchronous and synchronous transmissions, that convert between two different types of transmission

Prototyping—The process of quickly putting together a working model (a prototype) in order to test various aspects of a design, illustrate ideas or features and gather early user feedback. Prototyping uses programmed simulation techniques to represent a model of the final system to the user for advisement and critique. The emphasis is on end-user screens and reports.

Internal controls are not a priority item since this is only a model.

Proxy server—A server that acts on behalf of a user. Typical proxies accept a connection from a user, decide as to whether the user or client IP address is permitted to use the proxy, perhaps perform additional authentication, authentication and complete a connection to a remote destination on behalf of the user.

Public key cryptosystem—Used in data encryption, it uses an encryption key, as a public key, to encrypt the plaintext to the ciphertext. It uses a different decryption key, as a secret key, to decrypt the ciphertext to the corresponding plaintext. In contrast to a private key cryptosystem, the decryption key should be secret; however, the encryption key can be known to everyone. In a public key cryptosystem, the two keys are asymmetric, such that the encryption key is not equivalent to the decryption key.

Public key encryption—A cryptographic system that uses two keys: one is a public key, which is known to everyone, and the second is a private or secret key, which is only known to the recipient of the message

Public key infrastructure (PKI)—A series of processes and technologies for the association of cryptographic keys with the entity to whom those keys were issued

Q

Quality assurance (QA)—A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements (ISO/IEC 24765).

Queue—A group of items that are waiting to be serviced or processed **R**

Radio wave interference—The superposition of two or more radio waves resulting in a different radio wave pattern that is more difficult to intercept and decode properly

Random access memory (RAM)—The computer's primary working memory. Each byte of RAM can be accessed randomly regardless of adjacent

bytes.

Range check—Range checks ensure that data fall within a predetermined range

Rapid application development—A methodology that enables enterprises to develop strategically important systems faster, while reducing development costs and maintaining quality by using a series of proven application development techniques, within a well-defined methodology

Real-time processing—An interactive online system capability that immediately updates computer files when transactions are initiated through a terminal

Reasonable assurance—A level of comfort short of a guarantee, but considered adequate given the costs of the control and the likely benefits achieved

Reasonableness check—Compares data to predefined reasonability limits or occurrence rates established for the data

Reciprocal agreement—Emergency processing agreement between two or more enterprises with similar equipment or applications. Typically, participants

of a reciprocal agreement promise to provide processing time to each other when an emergency arises.

Record—A collection of related information treated as a unit. Separate fields within the record are used for processing the information.

Recovery point objective (RPO)—Determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time to which it is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.

Recovery strategy—An approach by an enterprise that will ensure its recovery and continuity in the face of a disaster or other major outage. Plans and methodologies are determined by the enterprise's strategy. There may be

more than one methodology or solution for an enterprise's strategy. Examples of methodologies and solutions include contracting for hot site or cold site, building an internal hot site or cold site, identifying an alternate work area, a consortium or reciprocal agreement, contracting for mobile recovery or crate and ship, and many others.

Recovery testing—A test to check the system's ability to recover after a software or hardware failure

Recovery time objective (RTO)—The amount of time allowed for the recovery of a business function or resource after a disaster occurs **Redundancy check**—Detects transmission errors by appending calculated bits onto the end of each segment of data

Redundant Array of Inexpensive Disks (RAID)—Provides performance improvements and fault-tolerant capabilities via hardware or software solutions, by writing to a series of multiple disks to improve performance and/or save large files simultaneously

Reengineering—A process involving the extraction of components from existing systems and restructuring these components to develop new systems or to enhance the efficiency of existing systems. Existing software systems thus can be modernized to prolong their functionality. An example of this is a software code translator that can take an existing hierarchical database system and transpose it to a relational database system. Computer-aided software

engineering (CASE) includes a source code reengineering feature.

Registration authority (RA)—The individual institution that validates an entity's proof of identity and ownership of a key pair

Regression testing—A testing technique used to retest earlier program abends or logical errors that occurred during the initial testing phase **Remote access service (RAS)**—Refers to any combination of hardware and software to enable the remote access to tools or information that typically reside on a network of IT devices. Originally coined by Microsoft when

referring to their built-in NT remote access tools, RAS was a service provided by Windows NT that allowed most of the services that would be available on a network to be accessed over a modem link. Over the years, many vendors have provided both hardware and software solutions to gain remote access to various types of networked information. In fact, most modern routers include a basic RAS capability that can be enabled for any dial-up interface.

Remote Procedure Call (RPC)—The traditional Internet service protocol widely used for many years on UNIX-based operating systems and supported by the Internet Engineering Task Force (IETF) that allows a program on one computer to execute a program on another (e.g., server). The primary benefit derived from its use is that a system developer need not develop specific procedures for the targeted computer system. For example, in a client-server arrangement, the client program sends a message to the server with appropriate arguments, and the server returns a message containing the results of the program executed. Common Object Request Broker

Architecture (CORBA) and Distributed Component Object Model (DCOM) are two newer object-oriented methods for related RPC functionality.

Repeaters—A physical layer device that regenerates and propagates electrical signals between two network segments. Repeaters receive signals from one network segment and amplify (regenerate) the signal to compensate for signals (analog or digital) distorted by transmission loss due to reduction of signal strength during transmission (i.e., attenuation).

Replication—In its broad computing sense, involves the use of redundant software or hardware elements to provide availability and fault-tolerant capabilities. In a database context, replication involves the sharing of data

between databases to reduce workload among database servers, thereby improving client performance while maintaining consistency among all systems.

Repository—The enterprise database that stores and organizes data **Request for proposal (RFP)**—A document distributed to software vendors,

requesting them to submit a proposal to develop or provide a software product

Requirements definition—A technique used in which the affected user groups define the requirements of the system for meeting the defined needs.

Some of these are business-, regulatory- and security-related requirements as well as development-related requirements.

Resilience—The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect **Return on investment (ROI)**—A measure of operating performance and efficiency, computed in its simplest form by dividing net income by the total investment over the period being considered

Reverse engineering—A software engineering technique whereby existing application system code can be redesigned and coded using computer-aided software engineering (CASE) technology

Ring configuration—Used in either token ring or fiber-distributed database interface (FDDI) networks, all stations (nodes) are connected to a multistation access unit (MSAU), which physically resembles a star-type topology. A ring configuration is created when these MSAUs are linked together in forming a network. Messages in this network are sent in a deterministic fashion from sender and receiver via a small frame, referred to as a token ring. To send a message, a sender obtains the token with the right priority as the token travels around the ring, with receiving nodes reading those messages addressed to it.

Ring topology—A type of local area network (LAN) architecture in which the cable forms a loop, with stations attached at intervals around the loop. In ring topology, signals transmitted around the ring take the form of messages.

Each station receives the messages and each station determines, on the basis of an address, whether to accept or process a given message. However, after receiving a message, each station acts as a repeater, retransmitting the message at

its original signal strength.

Risk—The combination of the probability of an event and its consequence (ISO/IEC 73)

Risk analysis—The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats. It often involves an evaluation of the probable frequency of a particular event, as well as the probable impact of that event.

Risk appetite—The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission.

Risk assessment—A process used to identify and evaluate risk and its potential effects. Includes assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

Risk evaluation—The process of comparing the estimated risk against given risk criteria to determine the significance of the risk. [ISO/IEC Guide 73:2002]

Risk management—The coordinated activities to direct and control an organization with regard to risk (in this International Standard the term

‘control’ is used as a synonym for ‘measure’). [ISO/IEC Guide 73:2002]

Risk mitigation—The management of risk through the use of countermeasures and controls

Risk tolerance—The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives **Risk transfer**—The process of assigning risk to another enterprise, usually through the purchase of an insurance policy or by outsourcing the service.

Also known as risk sharing.

Risk treatment—The process of selection and implementation of measures

to modify risk [ISO/IEC Guide 73:2002]

Rounding down—A method of computer fraud involving a computer code that instructs the computer to remove small amounts of money from an authorized computer transaction by rounding down to the nearest whole value denomination and rerouting the rounded off amount to the perpetrator's account

Router—A networking device that can send (route) data packets from one local area network (LAN) or wide area network (WAN) to another, based on addressing at the network layer (Layer 3) in the open systems interconnection (OSI) model. Networks connected by routers can use different or similar networking protocols. Routers usually are capable of filtering packets based on parameters, such as source address, destination address, protocol and network application (ports).

RSA—A public key cryptosystem developed by R. Rivest, A. Shamir and L.

Adleman used for both encryption and digital signatures. The RSA has two different keys, the public encryption key and the secret decryption key. The strength of RSA depends on the difficulty of the prime number factorization.

For applications with high-level security, the number of the decryption key bits should be greater than 512 bits.

Run-to-run totals—Provide evidence that a program processes all input data and that it processed the data correctly

S

Salami technique—A method of computer fraud involving a computer code that instructs the computer to slice off small amounts of money from an authorized computer transaction and reroute this amount to the perpetrator's account

Scheduling—A method used in the information processing facility (IPF) to determine and establish the sequence of computer job processing

Scope creep—Also called requirement creep; this refers to uncontrolled

changes in a project's scope. Scope creep can occur when the scope of a project is not properly defined, documented and controlled. Typically, the scope increase

consists of either new products or new features of already approved products. Hence, the project team drifts away from its original purpose. Because of one's tendency to focus on only one dimension of a project, scope creep can also result in a project team overrunning its original budget and schedule. For example, scope creep can be a result of poor change control, lack of proper identification of what products and features are required to bring about the achievement of project objectives in the first place, or a weak project manager or executive sponsor.

Screening routers—A router configured fi to permit or deny traffic based on a set of permission rules installed by the administrator

Secure Sockets Layer (SSL)—A protocol that is used to transmit private documents through the Internet. The SSL protocol uses a private key to encrypt the data that is to be transferred through the SSL connection.

Security administrator—The person responsible for implementing, monitoring and enforcing security rules established and authorized by management

Security awareness—The extent to which every member of an enterprise and every other individual who potentially has access to the enterprise's information understand:

• Security and the levels of security appropriate to the enterprise

• The importance of security and consequences of a lack of security

• Their individual responsibilities regarding security (and act accordingly) This definition is based on the definition for IT security awareness as defined in *Implementation Guide: How to Make Your Organization Aware of IT*

Security, European Security Forum (ESF), London, 1993

Security incident—A series of unexpected events that involves an attack or series of attacks (compromise and/or breach of security) at one or more sites.

A security incident normally includes an estimation of its level of impact. A limited number of impact levels are defined, and, for each, the specific

actions required and the people who need to be notified are identified.

Security policy—A high-level document representing an enterprise's information security philosophy and commitment

Security procedures—The formal documentation of operational steps and processes that specify how security goals and objectives set forward in the security policy and standards are to be achieved

Security testing—Ensuring that the modified or new system includes appropriate controls and does not introduce any security holes that might compromise other systems or misuses of the system or its information
Segregation/separation of duties (SoD)—A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets. Segregation/separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.

Sequence check—Verification that the control number follows sequentially and any control numbers out of sequence are rejected or noted on an exception report for further research. Can be alpha or numeric and usually utilizes a key field.

Sequential file—A computer file storage format in which one record follows another. Records can be accessed sequentially only. It is required with magnetic tape.

Service bureau—A computer facility that provides data processing services to clients on a continual basis

Service level agreement—An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines (SLA) minimum performance targets for a service and how they will be measured

Service set identifier (SSID)—A 32-character unique identifier attached to

the header of packets sent over a wireless local area network (WLAN) that acts as a password when a mobile device tries to connect to the basic service set (BSS). The SSID differentiates one WLAN from another so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plaintext from a packet, it does not

supply any security to the network. An SSID is also referred to as a network name, because it is a name that identifies a wireless network.

Servlet—A Java applet or a small program that runs within a web server environment. A Java servlet is similar to a common gateway interface (CGI) program, but unlike a CGI program, once started, it stays in memory and can fulfill multiple requests, thereby saving server execution time and speeding up the services.

Session border controller (SBC)—Provide security features for Voice-over Internet Protocol (VoIP) traffic similar to that provided by firewalls. SBCs can be configured to filter specific VoIP protocols, monitor for denial-of-service (DOS) attacks, and provide network address and protocol translation features.

Sign-on procedure—The procedure performed by a user to gain access to an application or operating system. If the user is properly identified and authenticated by the system's security, the user will be able to access the software.

Simple Object Access Protocol (SOAP)—A platform-independent formatted protocol based on extensible markup language (XML) enabling applications to communicate with each other over the Internet. Use of SOAP

may provide a significant security risk to web application operations since use of SOAP piggybacks onto a web-based document object model and is transmitted via Hypertext Transfer Protocol (HTTP) (port 80) to penetrate server firewalls, which are usually configured to accept port 80 and port 21

File Transfer Protocol (FTP) requests. Web-based document models define how objects on a web page are associated with each other and how they can

be manipulated while being sent from a server to a client browser. SOAP

typically relies on XML for presentation formatting and also adds appropriate HTTP-based headers to send it. SOAP forms the foundation layer of the web services stack, providing a basic messaging framework on which more abstract layers can build. There are several different types of messaging patterns in SOAP but, by far the most common is the Remote Procedure Call (RPC) pattern, in which one network node (the client) sends a request message to another node (the server), and the server immediately sends a response message to the client.

Slack time (float)—Time in the project schedule, the use of which does not affect the project's critical path; the minimum time to complete the project based upon the estimated time for each project segment and their relationships. Slack time is commonly referred to as "float" and generally is not "owned" by either party to the transaction.

SMART—Stands for specific, measurable, attainable, realistic and timely, generally used to describe appropriately set goals

Smart card—A small electronic device that contains electronic memory, and possibly an embedded integrated circuit. Smart cards can be used for a number of purposes including the storage of digital certificates or digital cash, or they can be used as a token to authenticate users.

Software—Programs and supporting documentation that enable and facilitate use of the computer. Software controls the operation of the hardware and the processing of data.

Source code—The language in which a program is written. Source code is translated into object code by assemblers and compilers. In some cases, source code may be converted automatically into another language by a conversion program. Source code is not executable by the computer directly.

It must first be converted into machine language.

Source documents—The forms used to record data that have been captured.

A source document may be a piece of paper, a turnaround document or an image displayed for online data input.

Source lines of code (SLOC)—Often used in deriving single-point software size estimations.

SPOOL (simultaneous peripheral operations online)—An automated function that can be based on operating system or application in which electronic data being transmitted between storage areas are spooled or stored until the receiving device or storage area is prepared and able to receive the information. SPOOL allows more efficient electronic data transfers from one device to another by permitting higher speed sending functions, such as internal memory, to continue on with other operations instead of waiting on the slower speed receiving device,

such as a printer.

Spyware—Software whose purpose is to monitor a computer user's actions (e.g., websites they visit) and report these actions to a third party, without the informed consent of that machine's owner or legitimate user. A particularly malicious form of spyware is software that monitors keystrokes to obtain passwords or otherwise gathers sensitive information, such as credit card numbers, which it then transmits to a malicious third party. The term has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Standard—A mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as International Organization for Standardization (ISO)

Standing data—Permanent reference data used in transaction processing.

These data are changed infrequently, such as a product price file or a name and address file.

Star topology—A type of local area network (LAN) architecture that utilizes a central controller to which all nodes are directly connected. With star topology, all transmissions from one station to another pass through the central controller which is responsible for managing and controlling all communication. The central controller often acts as a switching device.

Statistical sampling—A method of selecting a portion of a population, by

means of mathematical calculations and probabilities, for the purpose of making scientifically and mathematically sound inferences regarding the characteristics of the entire population

Storage area networks (SANs)—A variation of a local area network (LAN) that is dedicated for the purpose of connecting storage devices to servers and other computing devices. SANs centralize the process for the storage and administration of data.

Structured Query Language (SQL)—The primary language used by both application programmers and end users in accessing relational databases
Substantive testing—Obtaining audit evidence on the completeness, accuracy

or existence of activities or transactions during the audit period **Supply chain management (SCM)**—A concept that allows an organization to more effectively and efficiently manage the activities of design, manufacturing, distribution, service and recycling of products and services to its customers

Surge suppressor—Filters out electrical surges and spikes **Suspense file**—A computer file used to maintain information (transactions, payments, or other events) until the proper disposition of that information can be determined. Once the proper disposition of the item is determined, it should be removed from the suspense file and processed in accordance with the proper procedures for that particular transaction. Two examples of items that may be included in a suspense file are receipt of a payment from a source that is not readily identified or data that do not yet have an identified match during migration to a new application.

Switches—Typically associated as a data link layer device, switches enable local area network (LAN) segments to be created and interconnected, which also has the added benefit of reducing collision domains in Ethernet-based networks.

Synchronous transmission—Block-at-a-time data transmission

System software—A collection of computer programs used in the design, processing and control of all applications. The programs and processing routines that control the computer hardware, including the operating system and utility programs.

System testing—Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. System test procedures typically are performed by the system maintenance staff in their development library.

System development life cycle (SDLC)—The phases deployed in the development or acquisition of a software system. SDLC is an approach used to plan, design, develop, test and implement an application system or a major modification to an application system. Typical phases of the SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and postimplementation review.

System exit—Special system software features and utilities that allow the user to perform complex system maintenance. Use of system exits often permits the user to operate outside of the security access control system.

System flowchart—Graphic representations of the sequence of operations in an information system or program. Information system flowcharts show how data from source documents flow through the computer to final distribution to users. Symbols used should be the internationally accepted standard.

System flowcharts should be updated when necessary

T

Table look-up—Used to ensure that input data agree with predetermined criteria stored in a table

Tape management system (TMS)—A system software tool that logs, monitors and directs computer tape usage.

Telecommunications—Electronic communication by special devices over distances or around devices that preclude direct interpersonal exchange

Test data—Simulated transactions that can be used to test processing logic, computations and controls actually programmed in computer applications.

Individual programs or an entire system can be tested. This technique includes Integrated Test Facilities (ITFs) and Base Case System Evaluations (BCSEs).

Test programs—Programs that are tested and evaluated before approval into the production environment. Test programs, through a series of change control moves, migrate from the test environment to the production environment and become production programs.

Third-party review—An independent audit of the control structure of a service organization, such as a service bureau, with the objective of providing assurance to the users of the service organization that the internal control structure is adequate, effective and sound

Threat—Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm. A potential cause of an unwanted incident (ISO/IEC 13335).

Throughput—The quantity of useful work made by the system per unit of time. Throughput can be measured in instructions per second or some other unit of

performance. When referring to a data transfer operation, throughput measures the useful data transfer rate and is expressed in kbps, Mbps and Gbps.

Token—A device that is used to authenticate a user, typically in addition to a username and password. A token is usually a device the size of a credit card that displays a pseudo random number that changes every few minutes.

Token ring topology—A type of local area network (LAN) ring topology in which a frame containing a specific format, called the token, is passed from one station to the next around the ring. When a station receives the token, it is allowed to transmit. The station can send as many frames as desired until a predefined time limit is reached. When a station either has no more frames to send or reaches the time limit, it transmits the token. Token passing prevents data collisions that can occur when two computers begin transmitting at the

same time.

Topology—The physical layout of how computers are linked together.

Examples of topology include ring, star and bus.

Transaction—Business events or information grouped together because they have a single or similar purpose. Typically, a transaction is applied to a calculation or event that then results in the updating of a holding or master file.

Transaction log—A manual or automated log of all updates to data files and databases

Transmission Control Protocol/Internet Protocol (TCP/IP)—Provides the basis for the Internet; a set of communication protocols that encompass media access, packet transport, session communications, file transfer, electronic mail (email), terminal emulation, remote file access and network management.

Trap door—Unauthorized electronic exit, or doorway, out of an authorized computer program into a set of malicious instructions or programs **Trojan horse**—Purposefully hidden malicious or damaging code within an authorized computer program. Unlike viruses, they do not replicate themselves, but they can be just as destructive to a single computer.

Tunneling—Commonly used to bridge between incompatible hosts/routers or to

provide encryption, a method by which one network protocol encapsulates another protocol within itself. When protocol A encapsulates protocol B, a protocol A header and optional tunneling headers are appended to the original protocol B packet. Protocol A then becomes the data link layer of protocol B. Examples of tunneling protocols include IPSec, Point-to-point Protocol Over Ethernet (PPPoE), and Layer 2 Tunneling Protocol (L2TP).

Tuple—A row or record consisting of a set of attribute value pairs (column or field) in a relational data structure

Twisted pairs—A low-capacity transmission medium; a pair of small, insulated wires that are twisted around each other to minimize interference from other wires in the cable.

U

Unicode—A standard for representing characters as integers. Unicode uses 16 bits, which means that it can represent more than 65,000 unique characters; this is necessary for languages, such as Chinese and Japanese.

Uninterruptible power supply (UPS)—Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level

Unit testing—A testing technique that is used to test program logic within a particular program or module. The purpose of the test is to ensure that the internal operation of the program performs according to specification. It uses a set of test cases that focus on the control structure of the procedural design.

Universal Serial Bus (USB)—An external bus standard that provides capabilities to transfer data at a rate of 12 Mbps. A USB port can connect up to 127 peripheral devices.

User awareness—The training process in security-specific issues to reduce security problems; users are often the weakest link in the security chain.

Utility programs—Specialized system software used to perform particular computerized functions and routines that are frequently required during normal processing. Examples include sorting, backing up and erasing data.

Utility script—A sequence of commands input into a single file to automate a repetitive and specific task. The utility script is then executed, either automatically or manually, to perform the task. In UNIX, these are known as shell scripts.

V

Vaccine—A program designed to detect computer viruses

Validity check—Programmed checking of data validity in accordance with predetermined criteria

Value-added network (VAN)—A data communication network that adds processing services, such as error correction, data translation and/or storage to the basic function of transporting data

Variable sampling—A sampling technique used to estimate the average or total value of a population based on a sample; a statistical model used to project a quantitative characteristic, such as a monetary amount **Verification**—Checks that data are entered correctly

Virus—A program with the ability to reproduce by modifying other programs to include a copy of itself. A virus may contain destructive code that can move into multiple programs, data files or devices on a system and spread through multiple systems in a network.

Voice mail—A system of storing messages in a private recording medium which allows the called party to later retrieve the messages

Voice-over Internet Protocol (VoIP)—Also called IP Telephony, Internet Telephony and Broadband Phone, a technology that makes it possible to have a voice conversation over the Internet or over any dedicated Internet Protocol (IP) network instead of dedicated voice transmission lines

Vulnerability—A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events

Vulnerability analysis—A process of identifying and lassifying vulnerabilities

W

WAN switch—A data link layer device used for implementing various WAN technologies, such as asynchronous transfer mode, point-to-point frame relay solutions, and integrated services digital network (ISDN). These devices are typically associated with carrier networks providing dedicated WAN switching and router services to organizations via T-1 or T-3 connections.

Warm site—Similar to a hot site but not fully equipped with all of the necessary hardware needed for recovery

Waterfall development—Also known as traditional development, a procedure-focused development cycle with formal sign-off at the completion of each level

Web Services Description Language (WSDL)—A language formatted with extensible markup language (XML). Used to describe the capabilities of a web service as collections of communication endpoints capable of exchanging messages; WSDL is the language used by Universal Description, Discovery and Integration (UDDI). See also Universal Description, Discovery and Integration (UDDI).

White box testing—A testing approach that uses knowledge of a program/module's underlying implementation and code intervals to verify its expected behavior

Wide area network (WAN)—A computer network connecting different remote locations that may range from short distances, such as a floor or building, to extremely long transmissions that encompass a large region or several countries

Wide area network (WAN) switch—A data link layer device used for implementing various WAN technologies, such as asynchronous transfer mode, point-to-point frame relay solutions, and integrated services digital network (ISDN). WAN switches are typically associated with carrier networks providing dedicated WAN switching and router services to enterprises via T-1 or T-3 connections.

Wi-Fi Protected Access (WPA)—A class of systems used to secure wireless

(Wi-Fi) computer networks. WPA was created in response to several serious weaknesses researchers found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard

and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard but will not work with some older network cards. Both provide good security with two significant issues. First, either WPA or WPA2 must be enabled and chosen in preference to WEP; WEP is usually presented as the first security choice in most installation instructions. Second, in the "personal" mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical six-to eight-character passwords users are taught to employ.

Wired Equivalent Privacy (WEP)—A scheme that is part of the IEEE

802.11 wireless networking standard to secure IEEE 802.11 wireless networks (also known as Wi-Fi networks). Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP was intended to provide comparable confidentiality to a traditional wired network (in particular, it does not protect users of the network from each other), hence the name. Several serious weaknesses were identified by cryptanalysts, and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the weaknesses, WEP provides a level of security that can deter casual snooping.

Wiretapping—The practice of eavesdropping on information being transmitted over telecommunications links

X

X.25 Interface—An interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode on some public data networks

Note: The CISA candidate may also want to be familiar with ISACA's Glossary, which can be viewed at *www.isaca.org/glossary*. Also available is a list of CISA exam terminology in different languages, which can be

viewed at *www.isaca.org/examterm.*

ACRONYMS

The following is a list of common acronyms used throughout the CISA Review Manual. These may be defined in the text for clarity.

4GL

Fourth-generation language

ACID

Atomicity, consistency, isolation and durability

ACL

Access control list

AES

Advanced Encryption Standard

AH

Authentication header

AI

Artificial intelligence

AICPA

American Institute of Certified Public Accountants

ALE

Annual loss expectancy

ALU

Arithmetic-logic unit

ANSI

American National Standards Institute

API

Application programming interface

ARP

Address Resolution Protocol

ASCII

American Standard Code for Information Interchange

ASIC

Application-specific integrated circuit

ATDM

Asynchronous time division multiplexing

ATM

Asynchronous Transfer Mode

ATM

Automated teller machine

B-to-B

Business-to-business

B-to-C

Business-to-consumer

B-to-E

Business-to-employee

B-to-G

Business-to-government

BCI

Business Continuity Institute

BCM

Business continuity management

BCP

Business continuity plan

BCP

Business continuity planning

BDA

Business dependency assessment

BI

Business intelligence

BIA

Business impact analysis

BIMS

Biometric Information Management and Security

BIOS

Basic Input/Output System

BIS

Bank for International Settlements

Bit

Binary digit

BLP

Bypass label process

BNS

Backbone network services

BOM

Bill of materials

BOMP

Bill of materials processor

BPR

Business process reengineering

BRP

Business recovery (or resumption) plan

BSC

Balanced scorecard

C-to-G

Consumer-to-government

CA

Certificate authority

CAAT

Computer-assisted audit technique

CAD

Computer-assisted design

CAE

Computer-assisted engineering

CAM

Computer-assisted manufacturing

CASE

Computer-aided software engineering

CCK

Complementary Code Keying

CCM

Constructive Cost Model

CCTV

Closed-circuit television

CD

Compact disk

CD-R

Compact disk-recordable

CD-RW

Compact disk-rewritable

CDDF

Call Data Distribution Function

CDPD

Cellular Digital Packet Data

CEO

Chief executive officer

CERT

Computer emergency response team

CGI

Common gateway interface

CIA

Confidentiality, integrity and availability

CIAC

Computer Incident Advisory Capability

CICA

Canadian Institute of Chartered Accountants

CIM

Computer-integrated manufacturing

CIO

Chief information officer

CIS

Continuous and intermittent simulation

CISO

Chief information security officer

CMDB

Configuration management database

CMM

Capability Maturity Model

CMMI

Capability Maturity Model Integration

CNC

Computerized Numeric Control

COCOMO2

Constructive Cost Model

CODASYL

Conference on Data Systems Language

COM

Component Object Model

COM/DCOM Component Object Model/Distributed Component Object Model

COOP

Continuity of operations plan

CORBA

Common Object Request Broker Architecture

CoS

Class of service

COSO

Committee of Sponsoring Organizations of the Treadway Commission CPM

Critical Path Methodology

CPO

Chief privacy officer

CPS

Certification practice statement

CPU

Central processing unit

CRC

Cyclic redundancy check

CRL

Certificate revocation list

CRM

Customer relationship management

CSA

Control self-assessment

CSF

Critical success factor

CSIRT

Computer security incident response team

CSMA/CA

Carrier sense Multiple Access/Collision Avoidance

CSMA/CD

Carrier sense Multiple Access/Collision Detection

CSO

Chief security officer

CSU-DSU

Channel service unit/digital service unit

DAC

Discretionary access control

DASD

Direct access storage device

DAT

Digital audio tape

DBA

Database administrator

DBMS

Database management system

DCE

Data communications equipment

DCE

Distributed computing environment

DCOM

Distributed Component Object Model (Microsoft)

DCT

Discrete Cosine Transform

DD/DS

Data dictionary/directory system

DDL

Data Definition Language

DDN

Digital Divide Network

DDoS

Distributed denial of service

DECT

Digital Enhanced Cordless Telecommunications

DES

Data Encryption Standard

DFD

Data flow diagram

DHCP

Dynamic Host Configuration Protocol

DID

Direct inward dial

DIP

Document image processing

DLL

Dynamic link library

DMS

Disk management system

DMZ

Demilitarized zone

DNS

Domain name system

DoS

Denial of service

DRII

Disaster Recovery Institute International

DRM

Digital rights management

DRP

Disaster recovery plan

DRP

Disaster recovery planning

DSL

Digital subscriber lines

DSS

Decision support systems

DSSS

Direct Sequence Spread Spectrum

DTE

Data terminal equipment

DTR

Data terminal ready

DVD

Digital video disc

DVD-HD

Digital video disc-high definition/high density

DW

Data warehouse

EA

Enterprise architecture

EAC

Estimates at completion

EAI

Enterprise application integration

EAM

Embedded audit module

EAP

Extensible Authentication Protocol

EBCDIC

Extended Binary-coded for Decimal Interchange Code

EC

Electronic commerce

ECC

Elliptical Curve Cryptography

EDFA

Enterprise data flow architecture

EDI

Electronic data interchange

EER

Equal-error rate

EFT

Electronic funds transfer

EIGRP

Enhanced Interior Gateway Routing Protocol

EJB

Enterprise java beans

EMI

Electromagnetic interference

EMRT

Emergency response time

ERD

Entity relationship diagram

ERP

Enterprise resource planning

ESP

Encapsulating security payload

EVA

Earned value analysis

FAR

False-acceptance rate

FAT

File allocation table

FC

Fibre channels

FDDI

Fiber Distributed Data Interface

FDM

Frequency division multiplexing

FEA

Federal enterprise architecture

FEMA

Federal Emergency Management Association (USA)

FER

Failure-to-enroll rate

FERC

Federal Energy Regulatory Commission (USA)

FFIEC

Federal Financial Institutions Examination Council (USA)

FFT

Fast Fourier Transform

FHSS

Frequency-hopping spread spectrum

FIPS

Federal Information Processing Standards

FP

Function point

FPA

Function point analysis

FRAD

Frame relay assembler/disassembler

FRB

Federal Reserve Board (USA)

FRR

False-rejection rate

FTP

File Transfer Protocol

GAS

Generalized audit software

Gb

Gigabit

GB

Gigabyte

GID

Group ID

GIS

Geographic information systems

GPS

Global positioning system

GSM

Global system for mobile communications

GUI

Graphical user interface

HA

High availability

HD-DVD

High definition/high density-digital video disc

HDLC

High-level data link control

HIPAA

Health Insurance Portability and Accountability Act (USA)

HIPO

Hierarchy input-process-output

HMI

Human machine interfacing

HTML

Hypertext Markup Language

HTTP

Hypertext Transmission Protocol

HTTPS

Secured Hypertext Transmission Protocol

HW/SW

Hardware/software

I/O

Input/output

I&A

Identification and authentication

ICMP

Internet Control Message Protocol

ICT

Information and communication technologies

ID

Identification

IDE

Integrated development environment

IDEF1X

Integration Definition for Information Modeling

IDS

Intrusion detection system

IETF

Internet Engineering Task Force

IMS

Integrated manufacturing systems

IP

Internet protocol

IPF

Information processing facility

IPL

Initial program load

IPMA

International Project Management Association

IPRs

Intellectual property rights

IPS

Intrusion prevention system

IPSec

IP Security

IPX

Internetwork Packet Exchange

IR

Infrared

IRC

Internet relay chat

IrDA

Infrared Data Association

IRM

Incident response management

IS/DRP

IS disaster recovery planning

ISAKMP/

Internet Security Association and Key

Oakley

Management Protocol/Oakley

IS

Information systems

ISAM

Indexed Sequential Access Method

ISDN

Integrated services digital network

ISO

International Organization for Standardization

ISP

Internet service provider

IT

Information technology

ITF

Integrated test facility

ITGI

IT Governance Institute

ITIL

Information Technology Infrastructure Library

ITSM

IT service management

ITT

Invitation to tender

ITU

International Telecommunications Union

IVR

Interactive voice response

JIT

Just in time

Kb

Kilobit

KB

Kilobyte

KB

Knowledge base

KGI

Key goal indicator

KPI

Key performance indicator

KRI

Key risk indicator

L2TP

Layer 2 Tunneling Protocol

LAN

Local area network

LCP

Link Control Protocol

M&A

Mergers and acquisition

MAC

Mandatory access control

MAC

Message Authentication Code

MAC Address Media Access Control Address

MAN

Metropolitan area network

MAP

Manufacturing accounting and production

MIS

Management information system

MODEM

Modulator/demodulator

MOS

Maintenance out of service

MPLS

Multiprotocol label switching

MRP

Manufacturing resources planning

MSAUs

Multistation access units

MTBF

Mean time between failures

MTS

Microsoft’s Transaction Server

MTTR

Mean time to repair

NAP

Network access point

NAS

Network access server

NAS

Network attached storage

NAT

Network address translation

NCP

Network Control Protocol

NDA

Nondisclosure agreement

NFPA

National Fire Protection Agency (USA)

NFS

Network File System

NIC

Network interface card

NIST

National Institute of Standards and Technology (USA)

NNTP

Network News Transfer Protocol

NSP

Name Server Protocol

NSP

Network service provider

NT

New technology

NTFS

NT file system

NTP

Network Time Protocol

OBS

Object breakdown structure

OCSP

Online Certificate Status Protocol

ODC

On-demand computing

OECD

Organization for Economic Cooperation and Development

OEP

Occupant emergency plan

OLAP

Online analytical processing

OOSD

Object-oriented system development

ORB

Object request broker

OS

Operating system

OSI

Open Systems Interconnection

OSPF

Open Shortest Path First

PAD

Packet assembler/disassembler

PAN

Personal area network

PBX

Private branch exchange

PC

Personal computer/microcomputer

PCR

Program change request

PDCA

Plan-do-check-act

PDN

Public data network

PER

Package-enabled reengineering

PERT

Program Evaluation Review Technique

PICS

Platform for Internet Content Selection

PID

Process ID

PID

Project initiation document

PIN

Personal identification number

PKI

Public key infrastructure

PLC

Programmable logic controllers

PMBOK

Project Management Body of Knowledge

PMI

Project Management Institute

POC

Proof of concept

POP

Proof of possession

POS

Point of sale (or Point-of-sale systems)

POTS

Plain old telephone service

PPP

Point-to-point Protocol

PPPoE

Point-to-point Protocol Over Ethernet

PPTP

Point-to-Point Tunneling Protocol

PR

Public relations

PRD

Project request document

PRINCE2

Projects in Controlled Environments 2

PROM

Programmable Read-only Memory

PSTN

Public switched telephone network

PVC

Permanent virtual circuit

QA

Quality assurance

QAT

Quality assurance testing

RA

Registration authority

RAD

Rapid application development

RADIUS

Remote Access Dial-in User Service

RAID

Redundant Array of Inexpensive Disks

RAM

Random access memory

RAS

Remote access service

RBAC

Role-based access control

RDBMS

Relational database management system

RF

Radio frequencies

RFI

Request for information

RFID

Radio frequency identification

RFP

Request for proposal

RIP

Routing Information Protocol

RMI

Remote method invocation

ROI

Return on investment

ROLAP

Relational online analytical processing

ROM

Read-only memory

RPC

Remote procedure call

RPO

Recovery point objective

RSN

Robust secure network

RST

Reset

RTO

Recovery time objective

RTU

Remote terminal unit

RW

Rewritable

S/HTTP

Secure Hypertext Transfer Protocol

S/MIME

Secure Multipurpose Internet Mail Extensions

SA

Security Association

SAN

Storage area network

SANS

SysAdmin, Audit, Network, Security

SAS

Statement on Auditing Standards

SBx chain management

SCOR

Supply chain operations reference

SDLC

System development life cycle

SD/MMC

Secure digital multimedia card

SDO

Service delivery objective

SEC

Securities and Exchange Commission (USA)

SET

Secure electronic transactions

SIP

Service improvement plan

SLA

Service level agreement

SLIP

Serial Line Internet Protocol

SLM

Service level management

SLOC

Source lines of code

SMART

Specific, measurable, attainable, realistic, timely

SME

Subject matter expert

SMF

System management facility

SMTP

Simple Mail Transport Protocol

SNA

Systems network architecture

SNMP

Simple Network Management Protocol

SO

Security officer

SOA

Service-oriented architectures

SOAP

Simple Object Access Protocol

SOHO

Small office-home office

SOW

Statement of work

SPI

Security parameter index

SPICE

Software Process Improvement and Capability dEetermination

SPOC

Single point of contact

SPOOL

Simultaneous peripheral operations online

SQL

Structured Query Language

SSH

Secure Shell

SSID

Service set identifier

SSL

Secure Sockets Layer

SSO

Single sign-on

SVC

Switched virtual circuits

SYSGEN

System generation

TACACS

Terminal Access Controller Access Control System

TCO

Total cost of ownership

TCP

Transmission Control Protocol

TCP/IP

Transmission Control Protocol/Internet Protocol

TCP/UDP

Transmission Control Protocol/User Datagram Protocol

TDM

Time-division multiplexing

TELNET

Teletype network

TES

Terminal emulation software

TFTP

Trivial File Transport Protocol

TKIP

Temporal Key Integrity Protocol

TLS

Transport layer security

TMS

Tape management system

TP monitors

Transaction processing monitors

TQM

Total quality management

TR

Technical report

UAT

User acceptance testing

UBE

Unsolicited bulk email

UDDI

Universal description, discovery and integration

UDP

User Datagram Protocol

UID

User ID

UML

Unified Modeling Language

UPS

Uninterruptible power supply

URI

Uniform resource identifier

URL

Uniform resource locator

URN

Uniform resource name

USB

Universal Serial Bus

VLAN

Virtual local area network

VoIP

Voice-over IP

VPN

Virtual private network

WAN

Wide area network

WAP

Wireless Application Protocol

WBS

Work breakdown structure

WEP

Wired Equivalent Privacy

WLAN

Wireless local area network

WML

Wireless Markup Language

WORM

Write Once and Read Many

WP

Work package

WPA

Wi-Fi Protected Access

WPAN

Wireless personal area network

WSDL

Web Services Description Language

WWAN

Wireless wide area network

WWW

World Wide Web

X-to-X

Exchange-to-exchange

XBRL

Extensible Business Reporting Language

XML

Extensible Markup Language

XOR

Exclusive-OR

Xquery

XML query

XSL

Extensible Stylesheet Language

A

Acceptance testing, 116, 120, 128, 132, 133, 139, 152, 161, 162

Access control, 194, 263, 271, 272, 275

Access control list (ACL), 270

Access control table, 271

Access method, 166, 206, 261, 283

Access rights, 262, 272

Accountability, 83, 95, 185, 228, 250, 251, 305, 321

Accreditation, 171, 345

Accuracy, 42, 43, 218, 227, 237, 251

ACID, See Atomicity, Consistency, Isolation and Durability

ACLs, See Access control lists

Active attack, 328, 330

ActiveX, 29, 142, 333

Address space, 328

Addressing, 249, 250, 260,

Administrative controls, 21, 43

Advanced Encryption Standard (AES), 300, 303, 307

AES, See Advanced encryption standard

AICPA, See American Institute of Certified Public Accountants

ALE, See Annual loss expectancy

Alpha testing, 162

Alphanumeric, 267

Alternative processing, 220, 230, 232

Alternative routing, 214, 233

ALU, See Arithmetic-logic unit

American Institute of Certified Public Accountants (AICPA), 103

American National Standards Institute (ANSI), 32, 345

American Standard Code for Information Interchange (ASCII), 57, 279

Analog, 125

Annual loss expectancy (ALE), 212, 213

Anonymous File Transfer Protocol (Anonymous FTP), 291

ANSI, See American National Standards Institute

Anti-malware Software, 13, 332

Antivirus software, 39, 185, 245, 316, 318, 329, 343, 344

API, See Application programming interface

Applet, 29, 141, 290

Application Controls, 158

Application Development, 114, 131, 140, 142

Application layer, 279, 284, 298, 304

Application programmer, 69

Application programming interface (API), 34, 142, 143

Application system testing, 163

Application-specific integrated circuits (ASICs), 283

Arithmetic logic unit (ALU), 183, 350, 373

Artificial Intelligence, 39

ASCII, See American Standard Code for Information Interchange

ASICs, See Application-specific integrated circuits

Assembler language, 138

Asset value, 92

Asymmetric encryption, 302-304

Asynchronous time division multiplexing (ATDM), 286

Asynchonous transfer mode (ATM), 277

ATDM, See Asynchronous time division multiplexing

ATM, See Asynchronous transfer mode

Atomicity, Consistency, Isolation and Durability (ACID), 163

Antivirus software, 39, 249, 252, 318

Application-specific integrated circuits, 283

Attribute sampling, 53, 54

Audit approach, 21-23, 28, 44, 47, 51, 57, 58, 63, 115, 188, 200

Audit charter, 21, 22, 26, 27, 41, 65, 66

Audit documentation, 61

Audit evidence, 21, 23, 41, 46, 53-55, 57, 61, 130, 158, 274

Audit hooks, 58

Audit methodology, 60

Audit objective, 21, 50, 57, 60

Audit planning, 21-23, 28, 40, 43, 44, 46, 51, 60, 341

Audit program, 21, 49, 51, 57

Audit report, 60

Audit risk, 44, 46

Audit strategy, 20, 21, 27, 28, 49, 242, 348

Audit trail, 273

Authentication, 30, 35, 190, 264, 266, 302, 336

Authorization forms, 90

B

Backlog, 90, 156

Balanced scorecard (BSC), 77, 97, 107, 108

Balancing, 154, 158, 159

Bandwidth, 197, 200, 283-287, 305

Bar code, 35, 186, 219, 256

Baseband, 277

Base case, 351

Bastion host, 296, 297

Batch, 34, 154, 351

Batch balancing, 154

Batch Control, 34, 154

Batch processing, 65, 66

Batch registers, 154

BCP, See Business continuity planning

Beta testing, 162

BIA, See Business impact analysis

Bill of materials (BOM), 37

Binary code, 326

Biometrics, 268, 269

Black box testing, 162

Black swan event, 221

Bluetooth, 278, 317, 319-322

BOM, See Bill of materials

BPR, See Business process reengineering

Bridge, 51, 61, 143, 153, 331

Bring your own device (BYOD), 318

Broadband, 277, 287

Browser, 29, 30, 78, 184, 270, 289, 290, 294, 311, 319

Brute force attack, 272, 300

BSC, See Balanced scorecard

Budget, 50, 90, 122, 125, 129

Buffer, 142, 157, 208, 291, 298, 316, 327

Buffer overflow, 142

Bug, 57, 290

Business Continuity Planning (BCP), 100, 214, 219-230, 234

Business impact analysis (BIA), 82, 211-213, 228-230

Business process reengineering (BPR), 107, 122, 140, 143-145, 251

Business risk, 22, 44, 46, 135, 322

C

CA, See Certificate authority

Call-tracking, 307

CAM, See Computer-aided manufacturing

Capability maturity model (CMM), 87, 94, 101, 102, 103

Capability Maturity Model Integration (CMMI), 94

Capacity and Growth Planning, 105

Capacity Management, 197

Capacity planning, 197, 198

Carrier Sense Multiple Access/Collision Detection (CSMA/CD), 282

CASE, See Computer-aided software engineering

CDPD, See Cellular Digital Packet Data

Cellular Digital Packet Data (CDPD), 319

Central processing unit (CPU), 149, 183, 197, 326

Certificate authority (CA), 304, 305

Certificate revocation list (CRL), 304

Certification practice statement (CPS), 304

CGI, See Common gateway interface

Chain of custody, 342

Challenge/response, 267, 343, 344

Change control, 43, 133, 140, 142, 165, 166, 169, 170, 201, 298

Change Management, 99, 114

Channel service unit/digital service unit (CSU/DSU), 286

Check digit, 33, 116, 155

Checksum, 286, 307

CIM, See Computer-integrated manufacturing

Cipher, 256, 300, 303

Ciphertext, 299, 300-302

Circuit-switched network, 285

CIS, See Continuous and intermittent simulation

Client-server architecture, 292

Cloud Computing, 242, 310-314

CMM, See Capability maturity model

CMMI, See Capability maturity model integration

CNC, See Computerized numeric control

Coaxial cable, 214, 281, 282

COBIT, 20, 65, 66, 68, 74, 79, 106, 114, 191, 228

COCOMO, 126

Code Generators, 146

Coding standards, 116, 137

Cohesion, 137

Cold site, 179, 180, 232, 234

COM/DCOM, See Component Object Model/Distributed Component Object Model Common gateway interface (CGI), 138, 290, 330

Common Object Request Broker Architecture (CORBA), 142

Compensating control, 21, 43, 71, 90

Competence, 26, 27, 41

Compiler, 138

Completeness check, 153

Compliance testing, 44, 51-55, 164

Component Object Model/Distributed Component Object Model (COM/DCOM), 293

Computer operations, 65, 86, 156, 204, 258, 298, 325

Computer security incident response team (CSIRT), 340

Computer-assisted manufacturing (CAM), 41, 49, 56, 57, 61

Computer-aided software engineering (CASE), 55, 56, 141, 145, 146

Computer-integrated manufacturing (CIM), 37

Computerized numeric control (CNC), 37, 373

Concurrency, 87, 117

Constructive cost model (COCOMO), 126

Contingency planning, 35, 221, 261

Continuous and intermittent simulation (CIS), 58, 59

Continuous Auditing, 57, 58

Control account, 154

Control classifications, 41

Control group, 86, 90, 154, 165

Control matrix, 43, 88, 183, 252

Control Procedures, 156

Control risk, 21, 44, 45, 66, 98

Control self-assessment (CSA), 21, 62, 63, 94, 310

Conversion, 113, 114, 150, 166, 169, 347

CORBA, See Common Object Request Broker Architecture

Corporate governance, 44, 73

Corrective controls, 41, 105, 222

Coupling, 30, 137

CPM, See Critical path methodology

CPS, See Certification practice statement

CPU, See Central processing unit

Critical path method (CPM), 127, 128

CRL, See Certificate revocation list

CRM, See Customer relationship management

Cryptographic algorithm, 286

CSA, See Control self-assessment

CSIRT, See Computer security incident response team

CSMA/CD, See Carrier sense Multiple Access/Collision Detection

Customer relationship management, 37

Customer relationship management (CRM), 37, 40

Cyber attack, 225

Cybercrime, 76

D

DACs, See Discretionary Access Controls

Damage assessment team, 234

Data analysis, 48, 59, 79, 156, 342

Data center, 43, 60, 86, 193, 215, 220, 238, 239, 254, 258, 312, 316

Data Classification, 241, 242, 299, 347

Data Communication, 78, 195

Data communications equipment, 286

Data communications equipment (DCE), 286

Data control group, 90

Data Conversion, 113, 114, 166, 347

Data Dictionary, 206

Data Dictionary/Directory System, 206

Data dictionary/directory system (DD/DS), 206

Data Encryption, 241, 242, 299, 300, 347

Data Encryption Standard (DES), 36, 270, 286, 300, 303

Data Entry, 86

Data File Control Procedures, 6, 156

Data Integrity, 163

Data Leakage, 275

Data Management, 191

Data mining, 37, 59, 77, 189

Data owner, 89, 111, 244, 248, 259, 334

Data redundancy, 205, 209, 214

Data security, 69, 70, 189, 194, 205, 284, 291

Data structure, 56, 77, 168, 190, 207, 355

Data terminal equipment, 286, 352, 353, 372

Data terminal equipment (DTE), 286

Data Validation, 155

Data warehouse, 59, 251

Database administration, 43

Database administrator (DBA), 87, 88, 206

Database management system (DBMS), 205, 206, 217

Database specifications, 56, 133, 136, 137, 141

DBA, See Database administrator

DBMS, See Database management system

DCE, See Data communications equipment or Distributed computing environment DD, See Data dictionary

DD/DS, See Data Dictionary/Directory System

Deadlock, 208

Debugging, 57, 138, 165, 195, 328

Decentralization, 83

Decision support systems (DSS), 31, 159, 160, 174, 247, 312, 313

Decompiler, 143

Decryption, 277

Decryption key, 277, 300

DECT, See Digital Enhanced Cordless Telecommunications

Delta release, 201

Demilitarized zone (DMZ), 38, 243, 244, 297, 316, 338

Denial of service (DoS), 272, 306, 307, 321, 326, 327, 330, 331

Deployment, 113, 114, 166, 311, 347

DES, See Data Encryption Standard

Design and development, 115, 116, 128, 133, 136, 159, 278, 280

Detailed design, 128, 132, 135, 137, 145

DevOps, 143

Dial-up access controls, 343

DID, See Direct inward dial

Digital Enhanced Cordless Telecommunications, 320

Digital Enhanced Cordless Telecommunications (DECT), 320

Digital envelope, 303

Digital rights management, 260

Digital rights management (DRM), 260

Digital Signature, 243, 244, 272, 302, 303, 306, 307, 338

Digital subscriber lines (DSL), 271, 287

Direct inward dial (DID), 307

Disaster recovery planning (DRP), 214, 228-237

Disaster recovery procedures, 38, 209, 235

Discovery sampling, 53

Discrete cosine transform, 37

Discrete cosine transform (DCT), 37

Discretionary access controls (DACs), 259

Disk management systems, 192

Diskless workstations, 332

Distributed computing environment, 270, 293

Distributed computing environment (DCE), 270

Diverse routing, 214, 233

DLL, See Dynamic link library

DMZ, See Demilitarized zone

DNS, See Domain name system

Domain name system (DNS), 278, 357, 290

Downtime report, 200

DRM, See Digital rights management

DRP, See Disaster recovery planning

Dry-pipe sprinkling systems, 254

DSL, See Digital subscriber lines

DSS, See Decision support systems

DTE, See Data terminal equipment

Due Professional Care, 27

Dumb terminal, 357

Dynamic link library (DLL), 37

E

Ecommerce, 29, 30, 31

ecommerce architectures, 29

Ecommerce Requirements, 30

Ecommerce Risk, 30

Eavesdropping, 256, 302, 303, 306, 321, 327, 329, 330

EBCDIC, See Extended Binary-coded Decimal Interchange Code

ECC, See Elliptical curve cryptography

EDFA, See Enterprise data flow architecture

EDI, See Electronic data interchange

Edit controls, 155

Editing, 155, 156

EER, See Equal-error rate

EFT, See Electronic funds transfer

EIGRP, See Enhanced Interior Gateway Routing Protocol

EJB, See Enterprise Java Beans

Electromagnetic interference, 253

Electromagnetic interference (EMI), 253, 281

Electronic data interchange (EDI), 29-34, 86, 115, 117, 195, 214

Electronic Funds Transfer, 35

Electronic funds transfer (EFT), 195

Email, 34, 278, 307, 323, 327, 330, 331

Elliptical curve cryptography (ECC), 302

Embedded audit modules, 58, 137

Emergency management team, 229, 235

EMI, See Electromagnetic interference

Emulation, 271, 278, 291, 371

Encapsulation, 180, 208, 286, 304

Encapsulation security payload, 304

Encapsulation security payload (ESP), 43, 304

Encryption, 185, 190, 203, 241, 242, 272, 277, 295, 299-301, 318, 338, 347

Enhanced Interior Gateway Routing Protocol, 214

Enhanced Interior Gateway Routing Protocol (EIGRP), 214

Enterprise architecture, 68, 91, 178, 187, 191, 194, 205, 348

Enterprise architecture (EA), 91, 205

Enterprise data flow architecture, 77

Enterprise data flow architecture (EDFA), 77

Enterprise Java Beans, 142

Enterprise Java Beans (EJB) 142

Equal error rate, 268

Equal error rate (EER), 268

Error Reporting, 154

Escalation, 102, 104, 199, 202, 223, 224, 234, 237, 261, 335-337

Escrow, 101, 102, 151, 152, 196, 197, 230

ESP, See Encapsulation security payload

Ethernet, 149, 278, 281-283, 289, 320

Evidence, 19, 20, 54, 55, 61, 160, 241, 242, 340, 342, 347, 357

Exception report, 36, 155

Executable code, 143, 162, 208, 330

Expert Systems, 39, 40

Exposure, 256, 257, 262, 324

Extended Binary-coded for Decimal Interchange Code (EBCDIC), 279

External labeling, 157

Extensible Markup Language (XML), 30, 142, 278

External schema, 205

Extranet, 86, 180, 287

Extrapolation, 125, 342

F

Factorization, 301, 368

Failure-to-enroll rate (FER), 268

False-positive, 332

False-rejection rate (FRR), 268

Fast Fourier transform (FFT), 37

FDDI, See Fiber-Distributed Data Interface

FDM, See Frequency division multiplexing

Feasibility Study, 133

FER, See Failure-to-enroll rate

FFT, See Fast Fourier transform

Federated identity management, 274

Fiber-Distributed Data Interface (FDDI), 289

Fiber-optic, 214, 281, 285, 320

File server, 183

File Transfer Protocol (FTP), 214, 263, 288, 290, 291, 296, 297, 333, 339

Financial audit, 47

Financial Management Practices, 100

Fingerprint, 257, 268, 269

Firewall, 31, 295-298, 343

Firmware, 165, 192, 294, 315, 332

Flowcharts, 57

Follow-up, 159, 236, 273, 334

Forensics, 241, 242, 340, 342, 347

Fourth-generation language (4GL), 138, 140, 146, 159, 160

FPA, See Function point analysis

Frame relay, 174, 238, 271, 277, 286

Frequency division multiplexing (FDM), 286

Frequency of Rotation, 217

FTP, See Anonymous File Transfer Protocol or File Transfer Protocol Full duplex connection, 277

Function point analysis, 126

Function point analysis (FPA), 126, 37

Functional design specifications, 158

G

Gantt chart, 127, 148

Gateway, 31, 32, 34, 138, 235, 278, 284, 290, 296, 317, 330, 331

GEIT, See Governance of Enterprise IT

General audit procedure, 51

Generalized audit software, 51, 57, 163

Generally accepted standards of practice, 89

Geographical information system (GIS), 131

Gigabit, 150

Gigabyte, 319

GIS, See Geographical Information System

Global positioning system (GPS), 318

Global system for mobile communications (GSM), 319

Governance of Enterprise IT (GEIT), 68

GPS, See Global positioning system

Graphical user interface (GUI), 29, 125, 293

GSM, See Global System for Mobile Communications

GUI, See Graphical user interface

Guidelines, 19, 20, 25, 26, 79, 82, 188, 241, 42, 247, 347

H

Hacker, 185

Half duplex, 284

Hardened, 274, 275, 296, 298

Hardware Acquisition, 150

Hash, 42, 154, 301

HDLC, See High-level data link control

Health Insurance Portability and Accountability Act (HIPAA), 95, 185, 228, 250, 305

Help Desk, 89, 199

Hexadecimal, 342

Hierarchical database, 37, 206, 290

High-level data link control (HDLC), 286

HIPAA, See Health Insurance Portability and Accountability Act

Hiring practices, 98

Honeynet, 338

Honeypot, 338

HTML, See Hypertext Markup Language

HTTP, See Hypertext Transfer Protocol

HTTPS, See Secure Hypertext Transfer Protocol

Hub, 48, 282, 320

Hypertext Markup Language, 138, 349

Hypertext Markup Language (HTML), 138, 142, 289

Hypertext Transfer Protocol (HTTP), 34, 284, 288-290, 296, 297, 303

I

ICMP, See Internet control message protocol

IDE, See Integrated development environment

Identification and Authentication, 264

IEEE, See Institute of Electrical and Electronic Engineers

IETF, See Internet Engineering Task Force

Image Processing, 37

Impersonation, 328

Implementation phase, 138, 161

Implementation Strategies, 160, 332

IMS, See Integrated manufacturing systems

Inbound transactions, 32, 33, 115

Incident handling and response, 295

Incident Response, 223, 241, 242, 339, 342, 347

Independence, 25, 27, 41, 58-60, 62, 110, 111, 137, 146, 165, 205, 312

Industrial espionage, 190, 306, 325

Information processing facility (IPF), 85-89, 214, 215, 226, 255

Information Technology Infrastructure Library (ITIL), 79, 101, 102, 106, 204, 294

Infrared data association (IrDA), 278, 320

Inherent risk, 21, 22, 44, 45, 66

Initial program load, 193

Input Authorization, 153

Input controls, 156

Input/Origination Controls, 153

Institute of Electrical and Electronic Engineers (IEEE), 320

Insurance, 95, 185, 226, 228, 230, 233, 250, 305

Insurance Coverage, 230

Integrated development environment (IDE), 135, 138, 146

Integrated manufacturing systems (IMS), 37

Integrated services digital network (ISDN), 149, 271, 272, 277, 285-287, 320

Integrated test facilities (ITF), 58, 59

Integration, 94, 135, 143, 276

Inter-network Packet Exchange (IPX), 180, 284, 286

Interception, 175, 189, 190, 238, 299, 316, 317, 319

Internal control, 41, 44, 47-49, 51, 62, 63, 138

Internal labels, 157

Internal schema, 205, 206

International Organization for Standardization/Open Systems Interconnection (ISO/OSI), 288

International Telecommunications Union (ITU), 286, 305

Internet control message protocol (ICMP), 288, 326, 327, 336

Internet Engineering Task Force (IETF), 271, 288

Internet Protocol (IP), 34, 78, 180, 243, 244, 271, 286, 288

Internet service provider (ISP), 32, 271, 291

Internet of Things, 183, 322

Interoperability, 35, 107, 151, 279, 293

Interview, 50, 137, 165, 229

Intranet, 78, 143, 179, 180, 204, 225, 263, 287, 288, 323

Intruder, 194, 257, 267, 272, 297, 306, 327, 328, 330, 331, 338

Intrusion Detection, 337

IP, See Internet Protocol

IPF, See Information processing facility

IPX, See Inter-network Packet Exchange

IrDA, See Infrared Data Association

Irregularities, 51

IS Audit Function, 27

IS Budgets, 100

ISACA Code of Professional Ethics, 25, 26

ISACA IS Audit and Assurance Standards, 25, 26, 60

ISDN, See Integrated Services Digital Network

ISO 9001, 103, 109

ISO/OSI, See International Organization for Standardization/Open Systems Interconnection ISP, See Internet service provider

IT Performance, 68, 105, 347

ITAF, 20, 25, 26, 114

ITF, See Integrated test facilities

ITIL, See Information Technology Infrastructure Library

ITU, See International Telecommunications Union

J

Java, 29, 138, 142, 290, 330, 333

JavaEE, 91

Javascript, 138

Job description, 42, 85, 250, 256, 275

Job rotation, 99

K

Kerberos, 270

Kernel, 192, 193, 315

Key goal indicator (KGI), 98

Key performance indicator (KPI), 68, 98, 107

Key Personnel, 230

Key verification, 155

KGI, See Key goal indicator

KPI, See Key performance indicator

L

LAN, See Local area network

Last-mile circuit protection, 214

Latency, 213, 215, 244, 283, 291

LCP, See Link Control Protocol

Leased lines, 277, 287, 320

Legacy systems, 30, 31, 76, 217

Library Controls, 215

Limit check, 155, 156

Link Control Protocol (LCP), 286

Load balancing, 213, 283, 284, 291, 293, 297, 311

Local area network (LAN), 88, 263, 274, 275, 278, 281-284, 289-292

Logic bomb, 321

Logical Access Controls, 273

Logical security, 43, 47, 65, 194, 242, 247, 248, 258, 275, 348

Logon ID, 267

Long-haul network diversity, 214, 233

M

MACs, See Mandatory access control

MAC address, See Media Access Control Address

Machine language, 138, 350

Magnetic card readers, 35

Mainframe, 184, 187, 193, 275, 278, 284

Malware, 249, 317, 318, 326, 330-333

Management principles, 100, 123

Mandatory access controls, 259

Mandatory access controls (MACs), 259

Manual controls, 28, 144, 190

Manufacturing resources planning, 37

Manufacturing resources planning (MRP), 37

Masking, 334

Masquerading, 284, 327, 328

Master file, 32, 33, 154, 163, 164, 217, 229

Materiality, 21, 26, 44, 59, 60, 61

Media Access Control Address (MAC address), 174, 175, 280, 282

Memory dump, 138

Message digest, 300, 307

Message Modification, 328

Message switching, 32

Metadata, 30, 77, 205

Microchip, 185

Microcomputer, 146, 193, 278, 334

Microfiche, 217

Microsoft’s Transaction Server (MTS), 142

Middleware, 29-31, 193, 293, 294

Mirroring, 179, 181, 214, 231

Mobile Computing, 317

Mobile Devices, 317, 318

Modem, 32, 271, 272, 277, 286, 287, 297, 343, 344

Modulation, 277, 287

MPLS, See Multiprotocol label switching

MRP, See Manufacturing resources planning

MTBF, See Mean time between failures

MTS, See Microsoft’s Transaction Server

MTTR, See Mean time to repair

Multiplexing, 286, 287

Multiplexor, 286

Multiprotocol label switching (MPLS), 287

Multitiered, 29, 230, 345

N

N-tier, 293

Naming Conventions, 273

NAS, See Network access server

NAT, See Network address translation

National Institute of Standards and Technology (NIST), 38, 46, 75, 224, 225, 228, 300, 310, 312, 339

NCP, See Network Control Protocol

NDA, See Nondisclosure agreement

Network access server (NAS), 272

Network address translation (NAT), 297

Network administrator, 65, 66, 279, 291, 296, 331

Network Architecture, 263

Network connectivity, 140, 165, 234, 237, 287, 288

Network control, 101, 195, 235, 258, 275, 294,

Network Control Protocol (NCP), 286

Network interface card (NIC), 282, 283, 289, 320

Network Management, 88, 200, 288, 291, 292

Network manager, 287

Network Security, 13, 242, 330

Network service provider (NSP), 287, 288

Network standards and protocols, 271, 279

Neural networks, 39, 337

NIC, See Network interface card

NIST, See National Institute of Standards and Technology

Node, 39, 213, 287

Nondisclosure agreement (NDA), 335

Nonrepudiation, 35, 302, 321

Normalization, 342

NSP, See Network service provider

O

Object code, 71, 138, 196

Object-oriented system development (OOSD), 140, 141

Objectivity, 25, 26, 41, 58, 152

Occupant emergency plan (OEP), 224, 225

ODC, See On-demand computing

OECD, See Organization for Economic Cooperation and Development

OEP, See Occupant emergency plan

Office automation, 141

Offshore, 81, 100, 101, 103

Offsite Facility, 230

Offsite libraries, 215

Offsite Storage, 217, 219, 230

Offsite storage team, 235

OLAP, See Online analytical processing

On-demand computing (ODC), 281, 294,

Online analytical processing (OLAP), 77

Online programming facilities, 135

OOSD, See Object-oriented system development

Open Shortest Path First (OSPF), 214

Open system, 150, 280

Open Systems Interconnection (OSI), 279-286, 288, 289

Operational control, 43

Operations manager, 86, 334

Operator console, 195

Optical scanner, 35

Organization for Economic Cooperation and Development (OECD), 73

OSI, See Open Systems Interconnection

OSPF, See Open Shortest Path First

Outbound transactions, 32-34

Output analyzer, 138

Outsourcing, 40, 101-104

P

Packet, 34, 276-288, 296, 297, 305

Packet switching, 277, 283, 287, 305

Parallel simulation, 163

Parallel testing, 115, 116, 162, 165

Parity check, 157

Passive Attack, 306, 330

Password, 265, 267, 334

Paths of Logical Access, 262

PBX, See Private branch exchange

PDCA, See Plan-Do-Check-Act

PDNs, See Public data networks

Penetration testing, 57, 335, 337

Performance indicators, 68, 74, 77, 105, 107, 188, 265, 348

Performance Optimization, 106

Performance testing, 161

Peripherals, 86, 149, 184, 185, 187, 195, 266

Personal data, 28, 95, 316, 317

Personal identification number (PIN), 35, 36, 266, 319

PERT, See Program Evaluation Review Technique

Phreakers, 213

Physical Access Controls, 256

Physical layer, 195, 280, 283, 285, 286

Physical security, 35, 36, 56, 65, 147, 186, 248, 257, 312

Piggybacking, 257

PIN, See Personal identification number

Ping, 291, 326, 327

PingSweep, 336

PKI, See Public key infrastructure

Plaintext, 299, 300, 302

Plan-do-check-act (PDCA), 106, 107, 144

Plan Maintenance, 227

Point-of-sale Systems (POS), 35, 36, 174, 175

Point-to-point protocol (PPP), 286, 289

Policies, 61, 67 68, 79, 80, 89, 98, 99, 104, 157, 247, 276, 304, 317, 347

Polymorphism, 141, 332

Portfolio Management, 97

POS, See Point-of-sale System

Postimplementation, 370

PPP, See Point-to-point Protocol

Preventive control, 21, 23, 70, 115, 116, 144, 245, 247, 340, 344

Privacy, 35, 95, 186, 241, 242, 250, 251, 291, 310, 311, 347

Private branch exchange, 305

Private branch exchange (PBX), 305-307

Private key, 31, 301, 302, 304, 307

Problem escalation, 199

Problem Management, 198, 200

Procedures, 81, 154-156, 159, 170, 186, 187, 216, 217, 247, 336

Processing Controls, 155

Production software, 275

Professional competence, 41

Professional standards, 26, 41, 61

Program change control, 52

Program changes, 50, 69, 156, 170

Program Evaluation Review Technique (PERT), 127, 128, 174, 365, 375

Program logic, 145, 162, 164, 217, 275, 293

Programmed controls, 156

Programming languages, 138, 143, 146, 189, 205, 217, 311

Project Management, 19, 20, 49, 119-122, 129, 139, 347

Project Management Structure, 119

Project Management Techniques, 121

Project manager, 85, 121

Project team, 82, 120, 121, 124, 125, 129-131, 134, 139, 144, 145, 151, 152, 162, 167, 168, 172

Promotion Policies, 98

Protocol converters, 284

Protocol, 143, 200, 279, 286, 288-292

Prototyping, 139, 159

Proxy server, 179, 184, 238, 263, 296, 297

PSTN, See Public-switched telephone network

Public data networks (PDNs), 286

Public Key, 241, 242, 304, 347

Public key cryptosystem, 302

Public key encryption, 304

Public Key Infrastructure (PKI), 31, 241, 242, 304, 347

Public-switched telephone network (PSTN), 285, 306

Purchase Accounting System, 37

Q

QA, See Quality assurance

QAT, See Quality assurance testing

Quality assurance, 43, 62, 85, 109, 115, 116, 121

Quality assurance (QA), 43, 55, 85, 90, 108, 109, 121, 130, 142, 161, 201

Quality assurance testing, 161

Quality assurance testing (QAT), 161

Quality Management, 67, 68, 108, 109, 347

Quality management system, 103

Queue, 174, 293

R

RA, See Registration authority

RAD, See Rapid application development

Radio frequency identification (RFID), 185, 186

RAID, See Redundant Array of Inexpensive Disks

Range check, 115, 155

Rapid application development, 128, 134

Rapid application development (RAD), 134, 140, 143

Reactivation, 334

Read-only memory, 183

Read-only memory (ROM), 171, 183, 185, 332

Reasonable assurance, 26, 41, 42, 47, 52, 60, 76, 104, 195, 341

Reciprocal agreement, 232

Reconciliation, 36, 90, 154, 156

Recovery Alternatives, 10, 205, 232

Recovery point objective (RPO), 179, 181, 213, 216, 220, 228, 229, 231, 237

Recovery time objective (RTO), 179, 181, 213, 220, 228, 229, 231-233, 237, 238

Recurring problems, 187, 200

Redundancy, 148, 205, 209, 214, 219, 244, 280, 284

Redundancy check, 157

Redundant Array of Inexpensive Disks (RAID), 214, 215

Reengineering, 143, 145

Registration authority (RA), 304

Regression testing, 162

Regulations, 28, 67, 68, 95, 310, 347

Relational, 77, 163, 166, 206, 207, 208

Reliance, 53, 90, 140, 198

Remote Access, 11, 271, 272

Remote procedure calls (RPC), 142, 143, 293, 367, 369

Replication, 79, 181, 215, 216, 220, 231, 232

Repository, 69, 70, 77, 140, 146, 167, 183, 184, 189, 196, 197, 205, 217, 328

Request for information (RFI), 152

Request for proposal (RFP), 101, 149, 151-153

Requirements Definition, 133, 134

Residual risk, 47, 65, 66, 91, 93, 100, 231, 324, 340

Resource allocation, 129, 350

Restoration, 177, 178, 214, 215, 347

Restructuring, 101, 208

Retina scan, 269

Return on investment (ROI), 76, 123, 124, 130, 131, 134, 146, 171, 172

Reusability, 126, 140

Reverse Engineering, 143

RFI, See Request for information

RFID, See Radio frequency identification

RFP, See Request for proposal

Risk Analysis, 46, 93, 242

Risk assessment, 27, 44-47, 93, 135, 259, 260, 324

Risk Assessment Model, 158

Risk Assessment Techniques, 46

Risk Factors, 38, 160, 324

Risk Management Process, 47, 92

Risk Management Program, 92

Risk-based audit approach, 22, 44

RMI, See Remote Method Invocation

ROI, See Return on investment

ROM, See Read-only memory

Rotation, 217, 218

Router, 31, 34, 272, 277, 283, 286, 287, 296-298, 316, 320-331, 338

RPC, See Remote procedure calls

RPO, See Recovery point objective

RSA, 226, 243, 302, 303

RTO, See Recovery time objective

Run-to-run totals, 156

S

S/MIME, See Secure Multipurpose Internet Mail Extensions

Sabotage, 215, 321, 328

Salami technique, 329

Sample audit review file (SARF), 58, 59, 165

Sampling, 19-21, 52, 54, 298, 347

SARF, See Sample audit review file

Scalability, 34, 35, 101, 151, 213, 239, 279, 291, 293, 297, 311

Scanning, 37, 38, 57, 143, 216, 249, 268, 269, 331, 332, 336, 339

SCARF, See Systems Control Audit Review File

Scheduling and Time Reporting, 98

SCM, See Supply chain management

SCOR, See Supply Chain Operations Reference

Screening (HR), 262

Screening routers, 338

Script, 331

SD/MMC, See Secure digital multimedia card

Secure digital multimedia card (SD/MMC), 149

Secure hash algorithm (SHA), 300, 303

Secure Hypertext Transfer Protocol (HTTPS), 284, 303

Secure Multipurpose Internet Mail Extensions (S/MIME), 303, 304

Secure Shell (SSH), 291, 304

Secure Sockets Layer (SSL), 31, 284, 300, 303

Security Administration, 87, 271

Security Administrator, 89, 248

Security Awareness, 241, 242, 247, 323, 347

Security parameter index (SPI), 95, 304

Security Policy, 80, 81

Security software, 234, 275

Security Testing, 241, 242, 333, 347

Segmentation, 59, 88

Segregation of Duties, 88-90

Sequence checking, 57

Service Level Agreements (SLA), 43, 102, 103, 199, 203, 204, 313, 314

Servlet, 290

SHA, See Secure hash algorithm

Shadow IT, 298

Shareware, 196

Simple Mail Transport Protocol, 34, 288, 291

Simple Mail Transport Protocol (SMTP), 34, 288, 291, 307, 333

Simple Network Management Protocol, 200, 288, 292

Simple Network Management Protocol (SNMP), 200, 288, 292

Simple Object Access Protocol, 143, 278

Simple Object Access Protocol (SOAP), 143, 278

Simulator, 58, 195

Single sign-on, 243, 244, 270

Single sign-on (SSO), 270

Skeletonization (thinning), 37

Smart card, 35, 268

SMTP, See Simple Mail Transport Protocol

SNA, See Systems network architecture

Sniffing, 284, 308, 336

SNMP, See Simple Network Management Protocol

SOAP, See Simple Object Access Protocol

Social engineering, 185, 299, 326

Software Acquisition, 149, 150, 153

Software Licensing, 188, 196

Source documents, 57, 153-155, 217

Source lines of code (SLOC), 125, 126

Spam, 326, 327

Specific, measurable, attainable, realistic, timely (SMART), 76, 124, 131

SPI, See Security parameter index

Spoofing, 284, 296, 308, 327, 328, 331

Spyware, 185, 326, 329, 338

SQL, See Structured Query Language

SSH, See Secure shell

SSL, See Secure Sockets Layer

SSO, See Single sign-on

Staffing, 98, 204, 309

Standards, See Professional standards

Star-topology, 283

Statistical sampling, 44, 52, 53

Stealth, 336, 338

Steering Committee, 82, 83

Storage array, 211

Strategic Planning, 76

Stress testing, 161

Structured Analysis, 136

Structured programming, 137, 138

Structured Query Language (SQL), 146, 206, 208, 209, 296, 298, 335, 336

Stubs, 163, 258

Substantive Testing, 52

Supervision, 26, 37, 41, 74, 202, 252, 312, 325

Supply chain management (SCM), 37, 40, 151, 186

Supply Chain Operations Reference, 91

Supply Chain Operations Reference (SCOR), 91

Surge protectors, 253, 255

SvCs, See Switched virtual circuits

Swipe card, 257

Switched network, 32, 285, 318

Switched virtual circuits, 285

Switched virtual circuits (SVCs), 285

SYN, 326, 336

System Access, 258, 272

System control parameters, 156

System conversion, 56

System development process, 138, 139, 172

System Development Tools, 145

System exits, 334

System testing, 115, 116, 132, 138, 161-163

Systems administration, 85

Systems administrator, 86

Systems control audit review file (SCARF), 58, 165

Systems network architecture (SNA), 180, 271, 284, 291, 376

Systems programming, 43

T

Tagging, 164, 317

TCP/IP, See Transmission Control Protocol/Internet Protocol

TDM, See Time-division multiplexing

Technical reference documentation, 158

Technical support, 32, 43, 85, 101, 121, 151, 152, 194, 199, 217, 233, 305

Telecommuting, 287

Telnet, 289

Terminals, 153, 157, 197, 235, 256, 262, 274, 298, 333, 334

Termination, 99, 248

Test data, 57, 59, 116, 162, 164, 165, 195, 299

Test data generators, 165

Test Execution, 227

Test programs, 165

Testing phase, 115, 161, 169

TFTP, See Trivial File Transport Protocol

Thinning (skeletonization), 37

Threats, 92, 308, 309, 310, 317, 321, 324, 330

Time-division multiplexing, 286

Time-division multiplexing (TDM), 286

Timebox, 128

Timestamp, 302

TLS, See Transport Layer Security

Token ring, 283

Topology, 39, 87, 281-285, 289, 291, 296, 298, 313, 320, 336

Total risk, 45

TP, See Transaction processing

Tracing, 57, 105, 154, 164

Traffic analysis, 277, 330

Transaction authorization, 32, 88

Transaction flowchart, 158

Transaction log, 59, 154

Transaction processing (TP), 205, 293

Transborder Data Flow, 291

Transcription, 33, 115, 116, 155

Transmission Control Protocol/Internet Protocol (TCP/IP), 78, 200, 271, 280, 282, 284, 288, 289, 290-292, 320, 330

Transport Layer Security (TLS), 12, 300, 303

Triggering, 223, 237

Trivial File Transport Protocol, 214

Trivial File Transport Protocol (TFTP), 214, 288

Trojan horse, 162, 225, 331

Tunnel, 180, 243, 288, 304

Tuple, 206, 208

Two-tiered, 293, 294

U

UAT, See User acceptance testing

UDDI, See Universal description, discovery and integration

UDP, See User Datagram Protocol

UML, See Unified Modeling Language

Unicast, 287

Unicode, 336

Unified Modeling Language (UML), 141, 143

Uniform resource locator (URL), 289, 290

Uninterruptible power supply (UPS), 215, 223, 233

Unit testing, 161

Universal Description, Discovery and Integration (UDDI), 143

Universal serial bus (USB), 184, 185, 226, 268

UNIX, 184, 193, 250, 290, 296, 333, 336

UPS, See Uninterruptible power supply

Uptime, 103, 305

URL, See Uniform resource locator

USB, See Universal serial bus

User acceptance testing (UAT), 128, 131, 138, 139, 161, 162, 165

User Authorization Tables, 90

User Datagram Protocol (UDP), 284, 288, 296, 336

User ID, 264

User manuals, 55, 158

User Satisfaction, 105

Utility Programs, 195

V

Validity check, 115, 155

Value-added network (VAN), 32, 34

VAN, See Value-added network

Variable sampling, 53, 54

VB, See Visual Basic

Virtual private network (VPN), 271, 287, 288

Virus, 284, 318, 331, 339, 340

Voice recovery, 214, 233

Visual Basic (VB), 290, 331

Voice-over IP (VoIP), 214, 244, 305, 306, 318

VoIP, See Voice-over IP

Volume testing, 161

VPN, See Virtual private network

Vulnerability, 57, 92, 143, 220, 250, 273, 303, 306, 329, 330, 339

W

Warm sites, 232

Web servers, 30, 184, 303

Web Services Description Language (WSDL), 143

Web site, 326

Web-based EDI, 32

WEP, See Wired Equivalent Privacy

White box testing, 162

WHOIS, 336

Wi-Fi Protected Access (WPA), 13, 320,

Wired equivalent privacy (WEP), 13, 174, 175, 319, 320

Wireless local area network (WLAN), 319, 320

Wireless Personal Area Network (WPAN), 13, 278, 320

Wireless Wide Area Network (WWAN), 13, 278, 320

WLAN, See Wireless local area network

Work Papers, 51

Workstation, 34, 138, 153, 184, 185, 196, 257

Worms, 321, 326, 330, 331, 338

X

X.25, 277, 286, 287

XML, 30, 142, 143, 208, 270, 278

READY FOR YOUR CISA EXAM?

LET ISACA HELP YOU GET PREPARED

Successful Certified Information Systems Auditor® (CISA®) exam candidates know the importance of properly preparing for the challenging CISA exam. That is why they turn to ISACA's study resources and review courses—for the knowledge and expertise necessary to earn a CISA certification.

CISA book resources:

- CISA Review Manual 27th Edition
- CISA Review Questions, Answers & Explanations Manual 12th Edition

CISA database resources:

- CISA Review Questions, Answers & Explanations Database – 12 Month Subscription
- CISA Review Questions, Answers & Explanations Database CD-ROM

CISA review course:

- Chapter-sponsored Review Courses
- Accredited Training Review Courses
- Virtual Instructor-led Training

To learn more about ISACA's certification exam prep materials, visit *www.isaca.org/bookstore*.

CISA Certified Information Systems Auditor®
An ISACA® Certification

ISACA®

Document Outline

- Table of Contents
- About This Manual
- Overview
- Format of This Manual
- Preparing for the CISA Exam
- Using the CISA Review Manual
- Using the CISA Review Manual and Other ISACA Resources
- Chapter 1:
- Information System Auditing Process
- Overview
- Domain 1 Exam Content Outline
- Learning Objectives/Task Statements
- Suggested Resources for Further Study
- Self-assessment Questions
- Answers to Self-assessment Questions
- Part A: Planning
- 1.0 Introduction
- 1.1 IS Audit Standards, Guidelines and Codes of Ethics
- 1.2 Business Processes
- 1.3 Types of Controls
- 1.4 Risk-based Audit Planning
- 1.5 Types of Audits and Assessments
- Part B: Execution
- 1.6 Audit Project Management
- 1.7 Sampling Methodology
- 1.8 Audit Evidence Collection Techniques
- 1.9 Data Analytics
- 1.10 Reporting and Communication Techniques
- 1.11 Quality Assurance and Improvement of the Audit Process
- Case Study
- Answers to Case Study Questions
- Chapter 2:
- Governance and Management of IT
- Overview

- Domain 2 Exam Content Outline
- Learning Objectives/Task Statements
- Suggested Resources for Further Study
- Self-assessment Questions
- Answers to Self-assessment Questions
- Part A: IT Governance
- 2.0 Introduction
- 2.1 IT Governance and IT Strategy
- 2.2 IT-related Frameworks
- 2.3 IT Standards, Policies and Procedures
- 2.4 Organizational Structure
- 2.5 Enterprise Architecture
- 2.6 Enterprise Risk Management
- 2.7 Maturity Models
- 2.8 Laws, Regulations and Industry Standards Affecting the Organization
- Part B: IT Management
- 2.9 IT Resource Management
- 2.10 IT Service Provider Acquisition and Management
- 2.11 IT Performance Monitoring and Reporting
- 2.12 Quality Assurance and Quality Management of IT
- Case Study
- Answers to Case Study Questions
- Chapter 3:
- Information Systems Acquisition, Development and Implementation
- Overview
- Domain 3 Exam Content Outline
- Learning Objectives/Task Statements
- Suggested Resources for Further Study
- Self-assessment Questions
- Answers to Self-assessment Questions
- Part A: Information Systems Acquisition and Development
- 3.0 Introduction
- 3.1 Project Governance and Management
- 3.2 Business Case and Feasibility Analysis
- 3.3 System Development Methodologies
- 3.4 Control Identification and Design
- Part B: Information Systems Implementation
- 3.5 Testing Methodologies
- 3.6 Configuration and Release Management

- 3.7 System Migration, Infrastructure Deployment and Data Conversion
- 3.8 Post-implementation Review
- Case Study
- Answers to Case Study Questions
- Chapter 4:
- Information Systems Operations and Business Resilience
- Overview
- Domain 4 Exam Content Outline
- Learning Objectives/Task Statements
- Suggested Resources for Further Study
- Self-assessment Questions
- Answers to Self-assessment Questions
- Part A: Information Systems Operations
- 4.0 Introduction
- 4.1 Common Technology Components
- 4.2 IT Asset Management
- 4.3 Job Scheduling and Production Process Automation
- 4.4 System Interfaces
- 4.5 End-user Computing
- 4.6 Data Governance
- 4.7 Systems Performance Management
- 4.8 Problem and Incident Management
- 4.9 Change, Configuration, Release and Patch Management
- 4.10 IT Service Level Management
- 4.11 Database Management
- Part B: Business Resilience
- 4.12 Business Impact Analysis
- 4.13 System Resiliency
- 4.14 Data Backup, Storage and Restoration
- 4.15 Business Continuity Plan
- 4.16 Disaster Recovery Plans
- Case Study
- Answers to Case Study Questions
- Chapter 5:
- Protection of Information Assets
- Overview
- Domain 5 Exam Content Outline
- Learning Objectives/Task Statements
- Suggested Resources for Further Study

- Self-assessment Questions
- Answers to Self-Assessment Questions
- Part A: Information Asset Security and Control
- 5.0 Introduction
- 5.1 Information Asset Security Frameworks, Standards and Guidelines
- 5.2 Privacy Principles
- 5.3 Physical Access and Environmental Controls
- 5.4 Identity and Access Management
- 5.5 Network and End-point Security
- 5.6 Data Classification
- 5.7 Data Encryption and Encryption-related Techniques
- 5.8 Public Key Infrastructure
- 5.9 Web-based Communication Technologies
- 5.10 Virtualized Environments
- 5.11 Mobile, Wireless and Internet-of-things Devices
- Part B: Security Event Management
- 5.12 Security Awareness Training and Programs
- 5.13 Information System Attack Methods and Techniques
- 5.14 Security Testing Tools and Techniques
- 5.15 Security Monitoring Tools tand Techniques
- 5.16 Incident Response Management
- 5.17 Evidence Collection and Forensics
- Case Study
- Answer to Case Study Questions
- Appendix A: CISA Exam General Information
- Appendix B: CISA 2019 Job Practice
- Glossary
- Acronyms
- Index