

JONES & BARTLETT LEARNING

INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

Auditing IT Infrastructures for Compliance

MARTY M. WEISS AND MICHAEL G. SOLOMON

SECOND EDITION

JONES & BARTLETT LEARNING

INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

Auditing IT Infrastructures for Compliance

MARTY M. WEISS AND MICHAEL G. SOLOMON

SECOND EDITION





World Headquarters

Jones & Bartlett Learning

5 Wall Street

Burlington, MA 01803

978-443-5000

info@jblearning.com

www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

Copyright © 2016 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

The content, statements, views, and opinions herein are the sole expression of the respective authors and not that of Jones & Bartlett Learning, LLC. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement or recommendation by Jones & Bartlett Learning, LLC and such reference shall not be used for advertising or product endorsement purposes. All trademarks displayed are the trademarks of the parties noted herein. *Auditing IT Infrastructures for Compliance, Second Edition* is an independent publication and has not been authorized, sponsored, or otherwise approved by the owners of the trademarks or service marks referenced in this product.

There may be images in this book that feature models; these models do not necessarily endorse, represent, or participate in the activities represented in the images. Any screenshots in this product are for educational and instructive purposes only. Any individuals and scenarios featured in the case studies throughout this product may be real or fictitious, but are used for instructional purposes only.

This publication is designed to provide accurate and authoritative information in regard to the Subject Matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the service of a competent professional person should be sought.

Production Credits

Chief Executive Officer: Ty Field

President: James Homer

Chief Product Officer: Eduardo Moura

SVP, Curriculum Solutions: Christopher Will

Director of Sales, Curriculum Solutions: Randi Roger

Editorial Management: High Stakes Writing, LLC, Lawrence J. Goodrich, President

Copy Editor, High Stakes Writing: Kate Shoup

Product Manager: Rainna Erikson

Product Management Assistant: Edward Hinman

Production Manager: Tina Chen

Associate Production Editor: Kristen Rogers

Senior Marketing Manager: Andrea DeFronzo

Manufacturing and Inventory Control Supervisor: Amy Bacus
Composition: Gamut + Hue, LLC
Cover Design: Scott Moden
Rights & Media Manager: Joanna Lundein
Rights & Media Research Coordinator: Mary Flatley
Cover Image: © wongwean/Shutterstock
Printing and Binding: Edwards Brothers Malloy
Cover Printing: Edwards Brothers Malloy

ISBN: 978-1-284-09070-3

Library of Congress Cataloging-in-Publication Data

Weiss, Martin (Martin M.)

Auditing IT infrastructures for compliance / Martin Weiss, manager of Information Security Gurus, RSA, the Security Division of EMC. — Second edition.

pages cm

Includes index.

ISBN 978-1-284-09070-3 (pbk.)

1. Computer security. 2. Computer networks—Security measures. 3. Compliance auditing. I. Title.

QA76.9.A25W428 2016

005.8--dc23

2015020504

6048

Printed in the United States of America

19 18 17 16 15 10 9 8 7 6 5 4 3 2 1

Contents

Preface

Acknowledgments

PART ONE

The Need for Compliance

CHAPTER 1

The Need for Information Systems Security Compliance

What Is an IT Security Assessment?

What Is an IT Security Audit?

What Is Compliance?

How Does an Audit Differ from an Assessment?

Why Are Governance and Compliance Important?

Case Study: Enron

Case Study: WorldCom

What If an Organization Does Not Comply with Compliance Laws?

Case Study: TJX Credit Card Breach

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 1 ASSESSMENT

CHAPTER 2

Overview of U.S. Compliance Laws

Introduction to Public and Private Sector Regulatory Requirements

Federal Information Security Management Act

U.S. Department of Defense Requirements

Certification and Accreditation and Risk Management Framework

Cybersecurity

Sarbanes-Oxley Act

Gramm-Leach-Bliley Act

Health Insurance Portability and Accountability Act

Children's Internet Protection Act

Children's Online Privacy Protection Act

Family Educational Rights and Privacy Act

Payment Card Industry Data Security Standard

Red Flags Rule

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 2 ASSESSMENT

CHAPTER 3

What Is the Scope of an IT Compliance Audit?

What Must Your Organization Do to Be in Compliance?

Protecting and Securing Privacy Data

Designing and Implementing Proper Security Controls

What Are You Auditing Within the IT Infrastructure?

User Domain

Workstation Domain

LAN Domain

LAN-to-WAN Domain
WAN Domain
Remote Access Domain
System/Application Domain
Maintaining IT Compliance
Conducting Periodic Security Assessments
Performing an Annual Security Compliance Audit
Defining Proper Security Controls

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 3 ASSESSMENT

PART TWO

Auditing for Compliance: Frameworks, Tools, and Techniques

CHAPTER 4

Auditing Standards and Frameworks

Why Frameworks Are Important for Auditing
The Importance of Using Standards in Compliance Auditing
COSO
COBIT

Service Organization Control Reports

ISO/IEC Standards
ISO/IEC 27001 Standard
ISO/IEC 27002 Standard

NIST 800-53

Cybersecurity Framework

Developing a Hybrid Auditing Framework or Approach

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 4 ASSESSMENT

CHAPTER 5

Planning an IT Infrastructure Audit for Compliance

Defining the Scope, Objectives, Goals, and Frequency of an Audit
Identifying Critical Requirements for the Audit
Implementing Security Controls
Protecting Privacy Data
Assessing IT Security
Risk Management
Threat Analysis
Vulnerability Analysis
Risk Assessment Analysis: Defining an Acceptable Security Baseline Definition
Obtaining Information, Documentation, and Resources
Existing IT Security Policy Framework Definition
Configuration Documentation for IT Infrastructure
Interviews with Key IT Support and Management Personnel: Identifying and Planning
NIST Standards and Methodologies
Mapping the IT Security Policy Framework Definitions to the Seven Domains of a Typical IT Infrastructure
Identifying and Testing Monitoring Requirements
Identifying Critical Security Control Points That Must Be Verified Throughout the IT Infrastructure
Building a Project Plan
CHAPTER SUMMARY
KEY CONCEPTS AND TERMS

CHAPTER 5 ASSESSMENT

CHAPTER 6

Conducting an IT Infrastructure Audit for Compliance

Identifying the Minimum Acceptable Level of Risk and Appropriate Security Baseline Definitions

Organization-Wide

Seven Domains of a Typical IT Infrastructure

Gap Analysis for the Seven Domains

Identifying All Documented IT Security Policies, Standards, Procedures, and Guidelines

Conducting the Audit in a Layered Fashion

Performing a Security Assessment for the Entire IT Infrastructure and Individual Domains

Incorporating the Security Assessment into the Overall Audit Validating Compliance Process

Using Audit Tools to Organize Data Capture

Using Automated Audit Reporting Tools and Methodologies

Reviewing Configurations and Implementations

Verifying and Validating Proper Configuration and the Implementation of Security Controls and Countermeasures

Identifying Common Problems When Conducting an IT Infrastructure Audit

Validating Security Operations and Administration Roles, Responsibilities, and Accountabilities Throughout the IT Infrastructure

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 6 ASSESSMENT

CHAPTER 7

Writing the IT Infrastructure Audit Report

Executive Summary of an Audit Report

Summary of Findings

IT Security Assessment Results: Risk, Threats, and Vulnerabilities

Reporting on Implementation of IT Security Controls and Countermeasures

Per Documented IT Security Policy Framework

Privacy Data

IT Security Controls and Countermeasure Gap Analysis

Compliance Requirement

Risk, Threat, and Vulnerability Mitigation Requirement

Compliance Assessment Throughout the IT Infrastructure

Presenting Compliance Recommendations

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 7 ASSESSMENT

CHAPTER 8

Compliance Within the User Domain

Compliance Law Requirements and Business Drivers

Protecting Privacy Data

Implementing Proper Security Controls for the User Domain

Items Commonly Found in the User Domain

Separation of Duties

Least Privilege

Need to Know

Confidentiality Agreements

Employee Background Checks

Acknowledgment of Responsibilities and Accountabilities
Security Awareness and Training for New Employees
Information Systems Security Accountability
 Requiring That Human Resources Take a Lead Role
 Defining Accurate IT and IT Security Employee Job Descriptions
 Incorporating Accountability into Annual Employee Performance Reviews
Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines
Best Practices for User Domain Compliance
CHAPTER SUMMARY
KEY CONCEPTS AND TERMS
CHAPTER 8 ASSESSMENT

CHAPTER 9

Compliance Within the Workstation Domain
Compliance Law Requirements and Business Drivers
 Protecting Private Data
 Implementing Proper Security Controls for the Workstation Domain
Devices and Components Commonly Found in the Workstation Domain
 Uninterruptible Power Supplies
 Desktop Computers
 Laptops/Tablets/Smartphones
 Local Printers
 Modems and Wireless Access Points
 Fixed Hard Disk Drives
 Removable Storage Devices
Access Rights and Access Controls in the Workstation Domain
Maximizing C-I-A
 Maximizing Availability
 Maximizing Integrity
 Maximizing Confidentiality
Workstation Vulnerability Management
 Operating System Patch Management
 Application Software Patch Management
Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines
Best Practices for Workstation Domain Compliance
CHAPTER SUMMARY
KEY CONCEPTS AND TERMS
CHAPTER 9 ASSESSMENT

CHAPTER 10

Compliance Within the LAN Domain
Compliance Law Requirements and Business Drivers
 Protecting Data Privacy
 Implementing Proper Security Controls for the LAN Domain
Devices and Components Commonly Found in the LAN Domain
 Connection Media
 Networking Devices
 Server Computers and Services Devices
 Networking Services Software
LAN Traffic and Performance Monitoring and Analysis
LAN Configuration and Change Management
LAN Management, Tools, and Systems
Access Rights and Access Controls in the LAN Domain
Maximizing C-I-A

Maximizing Confidentiality
Maximizing Integrity
Maximizing Availability

Managing the Vulnerability of LAN Components
Operating System Patch Management
Application Software Patch Management

Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines

Best Practices for LAN Domain Compliance

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 10 ASSESSMENT

CHAPTER 11

Compliance Within the LAN-to-WAN Domain

Compliance Law Requirements and Business Drivers
Protecting Data Privacy
Implementing Proper Security Controls for the LAN-to-WAN Domain

Devices and Components Commonly Found in the LAN-to-WAN Domain

- Routers
- Firewalls
- Proxy Servers
- Demilitarized Zones
- Honeypots
- Internet Service Provider Connections and Backup Connections
- Intrusion Detection Systems/Intrusion Prevention Systems
- Data Loss/Leak Security Appliances
- Web Content Filtering Devices
- Traffic-Monitoring Devices

LAN-to-WAN Traffic and Performance Monitoring and Analysis

LAN-to-WAN Configuration and Change Management

LAN-to-WAN Management, Tools, and Systems

- FCAPS
- Network-Management Tools

Access Rights and Access Controls in the LAN-to-WAN Domain

- Maximizing C-I-A
- Minimizing Single Points of Failure
- Dual-Homed ISP Connections
- Redundant Routers and Firewalls
- Web Server Data and Hard Drive Backup and Recovery
- Use of Virtual Private Networks for Remote Access to Organizational Systems and Data

Penetration Testing and Validating LAN-to-WAN Configuration

- External Attacks
- Internal Attacks
- Intrusive Versus Nonintrusive Testing
- Configuration Management Verification

Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines

Best Practices for LAN-to-WAN Domain Compliance

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 11 ASSESSMENT

CHAPTER 12

Compliance Within the WAN Domain

Compliance Law Requirements and Business Drivers
Protecting Data Privacy

Implementing Proper Security Controls for the WAN Domain
Devices and Components Commonly Found in the WAN Domain
WAN Service Providers
Dedicated Lines/Circuits
MPLS/VPN WAN or Metro Ethernet
WAN Layer 2/Layer 3 Switches
WAN Backup and Redundant Links
WAN Traffic and Performance Monitoring and Analysis
WAN Configuration and Change Management
WAN Management Tools and Systems
Access Rights and Access Controls in the WAN Domain
Maximizing C-I-A
WAN Service Availability SLAs
WAN Recovery and Restoration SLAs
WAN Traffic Encryption/VPNs
WAN Service Provider SOC Compliance
Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines
Best Practices for WAN Domain Compliance

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 12 ASSESSMENT

CHAPTER 13

Compliance Within the Remote Access Domain

Compliance Law Requirements and Business Drivers
Protecting Data Privacy
Implementing Proper Security Controls for the Remote Access Domain
Devices and Components Commonly Found in the Remote Access Domain
Remote Users
Remote Workstations or Laptops
Remote Access Controls and Tools
Authentication Servers
VPNs and Encryption
Internet Service Provider WAN Connections
Broadband Internet Service Provider WAN Connections
Remote Access and VPN Tunnel Monitoring
Remote Access Traffic and Performance Monitoring and Analysis
Remote Access Configuration and Change Management
Remote Access Management, Tools, and Systems
Access Rights and Access Controls in the Remote Access Domain
Remote Access Domain Configuration Validation
VPN Client Definition and Access Controls
TLS VPN Remote Access Via a Web Browser
VPN Configuration Management Verification
Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines
Best Practices for Remote Access Domain Compliance

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 13 ASSESSMENT

CHAPTER 14

Compliance Within the System/Application Domain

Compliance Law Requirements and Business Drivers

Protecting Data Privacy
Implementing Proper Security Controls for the System/Application Domain
Devices and Components Commonly Found in the System/Application Domain
Computer Room/Data Center
Redundant Computer Room/Data Center
Uninterruptible Power Supplies and Diesel Generators to Maintain Operations
Mainframe Computers
Minicomputers
Server Computers
Data Storage Devices
Applications
Source Code
Databases and Privacy Data
System and Application Traffic and Performance Monitoring and Analysis
System and Application Configuration and Change Management
System and Application Management, Tools, and Systems
Access Rights and Access Controls in the System/Application Domain
Maximizing C-I-A
BCP and DRP
Access Controls
Database and Drive Encryption
System/Application Server Vulnerability Management
Operating System Patch Management
Application Software Patch Management
Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines
Best Practices for System/Application Domain Compliance

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 14 ASSESSMENT

PART THREE

Beyond Audits

CHAPTER 15

Ethics, Education, and Certification for IT Auditors

IT Auditing Career Opportunities
Professional Ethics and Integrity of IT Auditors
Codes of Conduct for Employees and IT Auditors
Employer-/Organization-Driven Codes of Conduct
Employee Handbook and Employment Policies
(ISC)² Code of Ethics
Certification and Accreditation for IT Auditing

IIA
ISACA
SANS Institute

CHAPTER SUMMARY

KEY CONCEPTS AND TERMS

CHAPTER 15 ASSESSMENT

APPENDIX A

Answer Key

APPENDIX B

Standard Acronyms

Glossary of Key Terms

[References](#)

[Index](#)

To my children, Annie, Ollie, Max and Kobe.

—Marty M. Weiss

To God, who has richly blessed me in so many ways

—Michael G. Solomon

Preface

Purpose of This Book

This book is part of the Information Systems Security & Assurance Series from Jones & Bartlett Learning (www.jblearning.com). Designed for courses and curriculums in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information-security principles packed with real-world applications and examples. Authored by professionals experienced in information systems security, they deliver comprehensive information on all aspects of this field. Reviewed word for word by leading technical experts, these books are not just current, but forward-thinking—putting you in a position to solve the cybersecurity challenges not just of today, but of tomorrow, as well.

Part 1 of this book identifies and explains what each of these compliance laws requires in regard to safeguarding business and consumer privacy data elements and the design and implementation of proper security controls. Once these safeguards and security control requirements are defined for your organization, you have a yardstick of measurement for conducting an audit of your IT infrastructure for compliance.

Part 2 presents how to audit an IT infrastructure for compliance based on the compliance laws themselves, on the need to protect and secure business and consumer privacy data, and on the need to have properly documented and implemented security controls within the organization. Auditing standards and frameworks are also presented, along with what must be audited within the seven domains of a typical IT infrastructure. In addition to discussing the planning and conduct of an audit, **Part 2** also reviews how to document what was identified during the audit and how to determine whether compliance requirements are being met throughout the IT infrastructure. Specific security controls and countermeasures are presented for each of the domains of a typical IT infrastructure.

Part 3 provides a resource for readers and students who desire more information on becoming skilled at IT auditing and IT compliance auditing. This final chapter provides additional content on ethics, education, professional certifications, and IT auditing certifying organizations.

This book not only addresses the tools and techniques for auditing IT infrastructure for compliance, it also examines the need. While much of the content is related to information security, the text considers the broader and higher-level principles around information governance and risk management. It brings together the fields of auditing, which has traditionally been seen as a function of accounting, and information technology.

Learning Features

The writing style of this book is practical and conversational. Each chapter begins with a statement of learning objectives. Step-by-step examples of information security concepts and procedures are presented throughout the text. Illustrations are used both to clarify the material and to vary the presentation. The text is sprinkled with Notes, Tips, FYIs, Warnings, and sidebars to alert the reader to additional helpful information related to the subject under discussion. Chapter Assessments appear at the end of each chapter, with solutions provided in the back of the book.

Chapter summaries are included in the text to provide a rapid review or preview of the material and to help students understand the relative importance of the concepts presented.

Audience

The material is suitable for undergraduate or graduate computer science majors or information science majors, students at a two-year technical college or community college who have a basic technical background, or readers who have a basic understanding of IT security and want to expand their knowledge.

Acknowledgments

It takes the work of many folks to get a book like this published. I'd like to first thank the many people behind the scenes, across different organizations, that I don't get to interact with, but who work so hard to make the text a reality. Throughout the process I was able to work firsthand with many great people who deserve acknowledgment. Carole Jelen is a fantastic literary agent I've had the pleasure of working with over the years. Larry Goodrich kept things smooth and on track. Rainna Erikson, the product manager, has been a joy to work with. A huge thank you as well to the editors: Kate Shoup on the copy side, and Jeff Parker on the technical side. A huge thank you to my family for all the support as I juggled various tasks. Lastly, I'd just like to thank the Academy.

Marty M. Weiss

I would like to thank Jeff T. Parker, the book's technical reviewer, and Kim Lindros, who managed the project, reviewed, and ferried all the pieces that flowed between me and Jones & Bartlett. You two make this stuff so much easier and added a lot to the book. Also, thanks so much to Carole Jelen with Waterside Productions for working so hard to make this happen.

I would also like to thank my wife Stacey and my sons Noah and Isaac, who make everything I do possible and fun. I can never thank them enough. So, to my three best friends, thanks again.

Michael G. Solomon

About the Authors

MARTY M. WEISS has years of experience in audit, information security, risk management, and compliance. Marty holds a BS in computer studies from the University of Maryland University College and an MBA from the Isenberg School of Management at the University of Massachusetts Amherst. He has several certifications, including Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), and CompTIA Security+. He has authored and coauthored over a half-dozen books on information technology. Occasionally he molds minds as an adjunct professor. Originally a Florida native, he now lives in New England somewhere between Boston and New York City.

MICHAEL G. SOLOMON, CISSP, PMP, CISM, is a full-time security speaker, consultant, and author who specializes in achieving and maintaining secure IT environments. An IT professional and consultant since 1987, he has worked on projects for more than 100 major companies and organizations. He is a former instructor in Kennesaw State University's computer science and information sciences (CSIS) department, where he taught courses on software project management, C++ programming, computer organization and architecture, and data communications. He holds an MS in mathematics and computer science from Emory University (1998) and a BS in computer science from Kennesaw State University (1987); he is currently pursuing a PhD in computer science at Emory University. He has also authored and contributed to many IT security books, including *Fundamentals of Communications and Networking* (Jones & Bartlett Learning, 2015), *Fundamentals of Information Systems Security* (Jones & Bartlett Learning, 2014), and *Security Strategies in Windows Platforms and Applications* (Jones & Bartlett Learning, 2011).

The Need for Compliance

CHAPTER 1

The Need for Information Systems Security Compliance

CHAPTER 2

Overview of U.S. Compliance Laws

CHAPTER 3

What Is the Scope of an IT Compliance Audit?

CHAPTER 1

The Need for Information Systems Security Compliance

N THE EARLY TO MID-2000s, many large corporations suffered public failures. Since then, a number of compliance laws have been introduced. Many of these laws and regulations place an increased responsibility on information technology (IT) staff. This increased responsibility ensures there are proper information system controls throughout the environment to provide the necessary security of customer data. In addition, these controls ensure the integrity of the systems upon which business processes run.

Compliance goes beyond just conforming to internal policies and standards. Compliance extends outside of the organization, mapping to external regulations and industry standards. Regular assessments and audits of the IT environment are important for ensuring compliance. Failure to comply with external regulations and industry standards can carry severe penalties. As a result, it is increasingly important to understand the methods by which an organization can be evaluated and the relationship between compliance and risk management and governance.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- What an IT security assessment is
- What an IT security audit is
- What compliance is
- How audits differ from assessments
- What the importance of governance and compliance is
- What the consequences of not complying with compliance laws are

Chapter 1 Goals

When you complete this chapter, you will be able to:

- Examine the role of an IT assessment
- Examine the role of IT auditing
- Compare the differences between an audit and an assessment
- Summarize compliance and explain why it is important

What Is an IT Security Assessment?

Assessing IT security is typically part of a larger security program within an organization. Specifically, an IT security assessment is a key activity that involves the management of **risk**—an uncertainty that might lead to a loss. Information systems provide numerous benefits and efficiencies within organizations. However, these benefits come with risks. A risk-based approach to managing information security involves the following:

- Identifying and categorizing the information and the information systems
- Selecting and implementing appropriate security **controls**—actions or changes to be applied to systems to reduce weaknesses or potential losses
- Assessing the controls for effectiveness
- Authorizing the systems by accepting the risk based upon the selected security controls
- Monitoring the security controls on a continual basis

This approach is a continual cycle as organizations evolve and as activities such as assessments and monitoring reveal gaps and ineffective controls relevant to requirements and acceptable levels of risk.

The benefits provided to organizations as a result of information technology involve complex systems and processes. These systems not only benefit organizations, but they have also become critical components to the success of the organization. As a result, the continued and secured operation of these systems contributes largely to that success.

To understand their effectiveness, organizations must assess security controls. Security controls include the physical, procedural, and technical mechanisms to safeguard systems. First, are they implemented? Second, are they functioning as expected? If so, are they producing the required results based on the security policy of an organization?

You should not use a security assessment simply as a method for proving the strength of system security or as a reason to immediately provide greater security. Rather, a security assessment should produce information required to do the following:

- Identify weaknesses within the controls implemented on information systems.
- Confirm that previously identified weaknesses have been remediated or mitigated.
- Prioritize further decisions to mitigate risks.
- Provide **assurance**, a level of confidence that effective controls are in place and that associated risks are accepted and authorized.
- Provide support and planning for future budgetary requirements.

The personnel who conduct security assessments can be internal or external to an organization. While the procedures for assessments may vary widely by organization, the **National Institute of Standards and Technology (NIST)**, the technology agency of the U.S. Department of Commerce, provides a framework for effective security assessment plans in NIST Special Publication 800-53A. This publication defines a recommended assessment procedure, which includes a set of assessment **objectives**, or goals. Each objective has a set of assessment methods, including examination, interview, and test; and each objective has a set of assessment objects, including specification, mechanism, activity, and individual.

An assessment objective includes one or more statements that are directly related to a corresponding control to determine the validity and effectiveness of the control. For example, consider a common control that most users of computer systems have experienced: being locked out of an information system or application after too many unsuccessful logon attempts. The following illustrates the relationship between the control and the assessment objectives, methods, and objects.

Unsuccessful Logon Attempts

Control: The system enforces a limit of four consecutive invalid access attempts on the same username within a period of 15 minutes. The system automatically locks the account for 30 minutes. Subsequently, four more consecutive invalid access attempts within a period of 15 minutes lock the account indefinitely, which requires manual intervention by the system administrator.

Assessment objectives:

- Determine if the system enforces the defined threshold of consecutive invalid access attempts.
- Determine if the system enforces the delayed logon after initial account lock.
- Determine if the system enforces the defined threshold for locking the account indefinitely.



TIP

NIST Special Publication 800-53 Appendix F contains a catalog of assessment procedures. You can tailor the assessment procedures for use in performing a security assessment. Appendix H provides a summary template of all assessment procedures contained in Appendix F.

Assessment methods and objects:

- Examine access control policy statement and procedures addressing failed logon attempts.
- Examine associated information system documentation and configuration settings.
- Examine associated information system log records.
- Test the automated mechanism implementing the access control policy for failed logon attempts.

Methods for Conducting a Security Control Assessment

You can use several methods to conduct an assessment of security controls:

- **Examination**—Verify, inspect, or review associated assessment objects to understand or obtain evidence to support the existence and effectiveness of the security control. Examples include reviewing security policies and procedures and observing physical security mechanisms.
- **Interview**—Discuss associated assessment objects with groups or individuals to understand or obtain evidence to support the existence and effectiveness of the security control. Interviews can include senior officials, information system owners, security officers, information system operators, and network administrators.
- **Test**—Put associated assessment objects under specific conditions to compare actual behavior with what is expected to obtain evidence to support the existence and effectiveness of the security control. Objects can include hardware or software mechanisms or system operations or administration activities. Examples include testing actual security configuration settings and conducting penetration tests.

Assessment objectives should be part of your organization's IT security assessment plan. After executing the plan, you can create a report. The IT security assessment report documents the findings of the assessment and provides the information necessary to determine the effectiveness of the controls. Senior management uses the report to provide assurance that risks are appropriate to the goals of the organization and to help create, if necessary, another document for an action plan based on the results of the assessment.

 **TIP**

It's helpful to create an executive summary document that quickly highlights the key findings and recommendations in a security assessment report.

Not all IT security assessments need to be comprehensive to cover all security controls or even all information systems. In fact, security assessments are often performed partially across controls and information systems. Although this chapter has laid out a best-practice framework for a comprehensive IT security assessment, security assessments vary in scope, depth, and breadth. The following is a list of some sample assessments you might encounter:

- Network security architecture review
- Review of security policies, procedures, and practices
- Vulnerability scanning and testing
- Physical security assessment
- Security risk assessment
- Social engineering assessment
- Application assessment

 **NOTE**

Penetration tests are commonly referred to as *pen tests*. The terms *black box*, *white box*, and *gray box* are also related. A black-box test makes no assumptions about the environment to be tested, whereas a white-box test provides complete knowledge and information, such as network diagrams, about the environment to be tested. Gray-box tests are variations between black-box and white-box tests.

Another common type of assessment, and one that seems to be more popularized in the media, is a penetration test. A **penetration test** is an assessment method that attempts to bypass controls and gain access to a specific system by simulating the actions of a would-be attacker. However, penetration tests operate under specific constraints and rules of engagement. So they don't truly simulate the process a real adversary might take.

As a result, a penetration test is not necessarily the best means by which to judge the security of an information system. The test helps an organization understand its systems and gain insight into the level of effort an attacker might need to go through to penetrate the system. Penetration tests often reveal weaknesses or easily exploited vulnerabilities within a system. It is not uncommon for penetration tests to be a catalyst for selling management on the need to invest more money and/or effort in information security.

What Is an IT Security Audit?

An IT security **audit** is an independent assessment of an organization's internal policies, controls, and activities. You use an audit to assess the presence and effectiveness of IT controls and to ensure that those controls are compliant with stated policies. In addition, audits provide reasonable assurance that organizations are compliant with applicable regulations and other industry requirements.

Many people view an audit as a function of accounting. This makes sense because audits are often a part of the examination of financial systems and records. Consider, however, how financial accounting has moved away from traditional paper ledgers and books to information computer systems. The integrity of information systems is vital to accurate financial reporting. The integrity of information systems plays an important role in preventing financial disasters, such as those that occurred with a couple large companies in the early 2000s. These companies were **Enron** and **WorldCom**, which are discussed in the case studies later in this chapter. Even beyond financial reporting, computer information systems have now become a valuable asset within organizations, and as a result need control and auditing.

There are many types of audits, such as the following:

- **Financial audits**—These determine whether an organization's financial statements accurately and fairly represent the financial position of the organization.
- **Compliance audits**—These determine if an organization is adhering to applicable laws, regulations, and industry requirements.
- **Operational audits**—These provide a review of policies, procedures, and operational controls across different departments to ensure processes are adequate.
- **Investigative audits**—These investigate company records and processes based on suspicious activity or alleged violations.
- **Information technology audits**—These address the risk exposures within IT systems and assess the controls and integrity of information systems.

In addition, organizations are finding that integrated audits are more appropriate. Again consider the reliance on IT systems for transactions, storage of data, and communications across all operational aspects of an organization. Next, consider that many organizations—especially those that process payment cards and those that are publicly traded—are required to comply with numerous laws and regulations. As a result, it makes sense to be able to cover multiple regulations from a single audit event and prevent audit inefficiencies by treating compliance, financial, operational, and IT audits as silos. Aside from duplicating efforts, audit requirements can overlap between the various types of audits. As a result, it begins to make sense that an IT audit includes elements of a regulatory compliance audit or an operational audit includes elements of a financial and IT audit.

The scope of an IT audit often varies, but can involve any combination of the following:

- **Organizational**—This examines the management control over IT and related programs, policies, and processes.
- **Compliance**—This pertains to ensuring that specific guidelines, laws, or requirements have been met.
- **Application**—This involves the applications that are strategic—for example, those typically used by finance and operations.
- **Technical**—This examines the IT infrastructure and data communications.

External or internal auditors typically perform IT security audits. In most large companies, the auditor is actually a team of auditors. An external auditor is independent of the organization and is often engaged from one of the big accounting and consulting firms. Publicly traded companies are required to engage external auditors. Internal auditors are employed by the organization that they audit. Unlike external auditors, internal auditors are not independent of the organization they audit. They directly report to the board of directors

or a subcommittee of the board of directors. This is important so as not to be influenced by management and to ensure the integrity and honesty of their findings. Organizations often outsource their internal audit functions to an external consulting firm.

FYI

Who are the “big” auditors? That list is shrinking, but by 2002, what was called the Big Five had become the Big Four. These are the largest accounting and professional service firms. The Big Four includes PricewaterhouseCoopers (known as PwC), Deloitte, Ernst & Young (known as EY), and KPMG. Arthur Andersen was dropped from the Big Five list as a result of the Enron collapse, for which they were the auditors. Arthur Andersen was indicted for obstruction of justice and subsequently ceased operations.

An effective IT security audit program should ultimately accomplish three goals:

- Provide an objective and independent review of an organization’s policies, information systems, and controls.
- Provide reasonable assurance that appropriate and effective IT controls are in place.
- Provide audit recommendations for both corrective actions and improvement to controls.

In many cases, external auditors do not advise the client as internal auditors would. External auditors are typically limited to providing information about gaps discovered and leading the client to accepted principles. Internal auditors can provide recommendations for improvements; however, they should never be involved in the design or implementation of any system or control.

What Is Compliance?

Despite being a relatively simple term, the term **compliance** has become something of an enigma within many organizations. Different people view and define compliance in different ways. This is evident across different industries, within the same industries, and even within organizations.

The Merriam-Webster Online dictionary defines compliance as “the act or process of complying to a desire, demand, proposal, or regimen or to coercion.” To comply is “to conform, submit, or adapt as required or requested.” In regard to IT compliance, compliance pertains to two broad areas: internal and external. *Internal compliance* refers to an organization’s ability to follow its own rules, which are typically based on defined policies. *External compliance* refers to the need or desire for an organization to follow rules and guidelines set forth by external organizations and initiatives. Although many external-compliance mandates are regulatory in nature, other compliance initiatives also include standards and guidelines that must be followed as set forth by industry regulations.

The credit card industry is a prime example, which developed a set of security standards in an attempt to provide self-regulation. The majority of compliance mandates are, however, laws and regulations. There are numerous compliance mandates to which organizations may be required to adhere. In most cases, regulations do not provide specifics and are open for interpretation. Compliance frameworks, such as **Control Objectives for Information and Related Technology (COBIT)**, and standards, such as NIST, help interpret how to comply with the regulations.

Unlike a simple traffic law, such as the requirement to stop at a red light, compliance laws and regulations are not always so clear. This is often another source of frustration for those with the responsibility of helping an organization comply. The general steps to meeting compliance include the following:

1. Interpret the regulation and how it applies to the organization.
2. Identify the gap or determine where the organization stands with the compliance mandate.
3. Devise a plan to close the gap.
4. Execute the plan.

 **NOTE**

Meeting compliance often includes implementing mechanisms to prove that an organization has properly executed its plan.

Compliance is closely related to **risk management** and **governance** on all levels, be it technical, procedural, or strategic. Risk management seeks to mitigate risk through controls. For example, an organization identifies, evaluates, and takes action to lessen its risk. Compliance helps risk management by verifying that the desired controls are in place. Governance seeks to better run an organization using complete and accurate information and management processes or controls. For example, a sound security policy and comprehensive procedures are in place to implement the policy.

Compliance helps governance by ensuring such information and controls also satisfy applicable standards or regulations. On a strategic level, compliance ensures an organization can effectively meet organizational goals and objectives as planned. This means IT must ensure it is capable of delivering services to satisfy business needs and to stay compliant with external laws and regulations.

How Does an Audit Differ from an Assessment?

Although there seem to be many similarities between an audit and assessment, there are some stark differences. One is the mindset people tend to have about the word *audit*. This word brings to mind thoughts of distrust and punishment. Regardless of whether these feelings are justified, these thoughts are based on several outcomes that can result from an audit:

- **Failure**—Audits are typically more clear-cut in the sense of pass or fail. It is possible to fail an audit, but most people don't think of an assessment in terms of pass or fail. Rather, you might see an assessment as an opportunity to assess the current state and make improvements as necessary.
- **Blame**—Audit findings might place blame on specific individuals or groups within an organization. Assessments, on the other hand, are nonattributive. That is, they don't view an individual as being directly responsible for a poor finding. Many organizations use assessments to prepare for audits. Assessments provide a chance for improvement in a more comfortable and productive environment that helps facilitate the goals of the organization.
- **Consequences**—Audits can have consequences, many of which are negative. Consider

that an organization can fail an audit and, subsequently, have blame attributed to an individual or group. In addition, noncompliance with regulatory and industry standards can carry stiff penalties. The consequences of failing an audit can create a sense of fear, whereas an assessment simply identifies gaps to improve security operations and achieve goals.

Security auditing, in general, must follow a more rigid approach and process over a security assessment. This is a key point, especially when you consider that an audit is an assessment. Moreover, an audit contains the following unique characteristics:

- Auditors should never be involved in the auditing of processes, systems, or applications that they themselves designed or implemented.
- Audits are an independent evaluation. A security assessment may also be conducted independently, but it is not necessary. Many organizations use a combination of both.
- Audits follow a rigorous approach and are conducted according to accepted principles. This also requires that auditors be qualified. The approach taken for an assessment can fall across a wide spectrum, but in many cases, they have taken a cue from audits with well-defined approaches and frameworks.
- In the event an organization passes an audit, the organization typically receives some type of certification or confirmation. This is not the case for assessments.
- An audit is concerned about past results and performance, whereas an assessment considers previous and current results as well as expected performance.

You might find it helpful to evaluate a security audit and security assessment in more personal terms. Consider, for example, your own financial situation. When was the last time you personally assessed your financial state? Are you comfortable with your current situation? Are you on track to meet long-term goals? You can use many different tools and materials to do this yourself. Or you can hire a financial consultant or tax advisor to look at your situation, set goals, and identify gaps that exist in meeting those goals. Now imagine the U.S. Internal Revenue Service (IRS) knocking on your door to audit you. Granted, an individual IRS audit seems more adversarial. Keep in mind that is why companies go through audits in the first place. A successful audit enables a business or organization to be more profitable and/or successful without risk of penalties or being deemed incompliant.

Why Are Governance and Compliance Important?

Without proper governance in place, an organization can have neither effective risk management nor compliance. A common theme thus far has been the reliance on IT throughout the organization. As a result, IT can have a tremendous impact on either the success or failure of an organization. The interest in formally governing the use and application of IT should come as no surprise. IT is now woven into the fabric of business and has made organizations dependent on information and the systems that help generate and store information. In addition, IT will continue to provide opportunities for competitive advantage and reduction of costs throughout the organization. On the other hand, IT systems are subject to numerous threats that continue to evolve and seek to exploit vulnerabilities.

At a fundamental level, internal compliance to corporate policies is critical to the success of any business. Risk management means deeming some risks acceptable so a company may accomplish its business goals. Compliance, therefore, embraces the organizational mission,

and noncompliance can harm or even impede business.

Regulatory compliance benefits organizations, consumers, and shareholders. Regulatory compliance protects the reputation and integrity of the organizations that are required to comply. It considers the interests of the consumer and shareholders. Regulatory compliance also has a farther-reaching economic impact on ensuring public confidence in organizations and capital markets.

Case Study: Enron

Enron Corporation was a U.S.-based energy company that at one point was the seventh-largest company in the United States and the largest trader of natural gas and electricity in the country. Enron came about in the mid-1980s, focusing on the natural gas market. By the 1990s, it had pursued a diversification strategy to achieve growth. Subsequently, Enron got involved with trading and ownership in electric, coal, steel, paper, water, and broadband capacity.

Enron collapsed in 2001 and filed bankruptcy, which at the time was the largest bankruptcy in history. The collapse was a result of a complex and methodical accounting scandal. The fallout was massive, resulting in thousands of employees who were laid off and who lost their life savings plans that were tied to the company's stock. In addition, shareholders saw a loss of \$11 billion. Economically, the disaster perpetuated a lack of trust in the stock market and eroded public confidence.

NOTE

WorldCom would go on to surpass Enron as the largest bankruptcy. Ultimately, it was the Enron fiasco that led to the downfall of Arthur Andersen as one of the largest auditing and consulting firms.

Enron's auditing firm, Arthur Andersen, had attested to Enron's financial health for years, despite widespread fraud and hidden losses at Enron. In addition, the auditing and consulting firm assisted Enron in deal structuring and other consultative practices. Enron paid Arthur Andersen a combined \$52 million in consulting fees in the year 2000 alone. Arthur Andersen was eventually convicted of obstruction of justice as a result of shredding paper documents and destroying electronic documents related to their client. Arthur Andersen's involvement with Enron also led to the discovery of other audit discrepancies, including those at WorldCom.

Although complex and occurring over a period of many years, investigative findings discovered that Enron used several complicated and questionable accounting methods, including the following:

- Enron had reduced its tax payments and inflated its income and profits.
- Enron had increased its stock price and credit ratings.
- Enron had hidden losses in off-balance sheet subsidiaries.
- Enron employees funneled money to themselves and acquaintances.
- Enron's financial condition was misrepresented in public reports.

The Enron board of directors was faulted on several accounts. One of these was not being involved in the examination of terms related to moving debt off the company's balance sheets. They missed the chance to uncover fundamental flaws in the accounting practices at

the company. A report written by the special committee investigating Enron described what went wrong with management: “We found a systematic and pervasive attempt by Enron’s management to misrepresent the Company’s financial condition.” Enron’s culture was one that seemed to cast aside traditional controls. In fact, the investigating committee also stated that Enron had an “across-the-board failure of controls and ethics at almost every level of the company.” The report continued, describing “a flawed idea, self-enrichment by employees, inadequately designed controls, poor implementation, inattentive oversight, simple (and not so simple) account mistakes, and overreaching in a culture that appears to have encouraged pushing the limits.”

Enron has become in many ways the premier symbol of fraud, corruption, and audit failure. The scandal also resulted in a host of new regulations and legislation being enacted, including the **Sarbanes-Oxley Act**. This act addresses many of the shortcomings and lessons learned from the Enron scandal.

The following are some questions for further thought and discovery:

- How do a company’s acquisitions relate to risk management and governance?
- The Enron scandal resulted in steps to improve standards, controls, and accountabilities. How much do morals contribute to such events and what can be done to address this issue?
- What financial incentives may have been in place for Enron’s consulting firm to perhaps have lax auditing standards?
- Given the large sums paid on consultancy fees, is it possible that talented auditors are focused on consulting while less-experienced employees audit?
- How might a control framework for IT that is more closely aligned with business processes have prevented this?
- How could adequate controls on IT systems and financial applications have helped?
- Do you think that controls designed to prevent or detect fraud were in place? How important is the monitoring of such controls, and how should access be controlled?

Case Study: WorldCom

Prior to filing bankruptcy in 2002, WorldCom was the second largest telecommunications company in the world. It handled Internet data traffic globally and accounted for more international voice traffic than any other company.

WorldCom grew quickly from its modest beginning in 1983, and achieved its tremendous growth through 65 acquisitions. In the 1990s, the company made some large acquisitions, including MCI Communications. Through this period, WorldCom spent approximately \$60 billion and accumulated approximately \$41 billion in debt. The MCI acquisition was the largest merger in U.S. history at the time.

The market value of WorldCom continued to grow substantially through these acquisitions, and high expectations continued to be placed on the company. This generated pressure to keep the stock price at elevated levels, which in turn allowed WorldCom to continue its acquisition spree. A proposed merger in 2000 with Sprint would have eclipsed the merger with MCI; however, the merger was disapproved and WorldCom started to unravel. In an attempt to maintain its earnings, WorldCom liberally interpreted accounting rules to make its financial statements seem profitable. The company soon moved from liberal interpretation into outright fraud by creating false entries.

A team of internal auditors became suspicious over numerous financial oddities and began investigating, but the auditors encountered problems. They tried to discuss financial

irregularities with WorldCom's external auditors, Arthur Andersen, who did not fully cooperate. Responsible to the WorldCom chief financial officer (CFO) at the time, the internal audit group raised issues with the CFO but was pressured to stop. The internal auditors persisted and eventually uncovered what would become the largest account fraud in U.S. history.

How could this have happened, and what were some of the events and situations that led to this mess?

- The board of directors became simply a “rubber stamp.”
- The board of directors allowed the chief executive officer (CEO) and CFO of WorldCom to have unfettered power.
- WorldCom acquired many companies without a strategy for linking them properly.
- The board of directors approved deals worth billions of dollars with little discussion.
- Little oversight of debt accumulation existed.
- Little oversight of company loans made to the CEO existed.
- The company lacked internal controls and transparency.
- External consultants failed to apply techniques consistent with their risk rating of the company.
- Internal auditing was underqualified and focused on nonauditing activities.

Consider the questions previously discussed in the Enron case. What parallels can you draw between these two disasters? How can information technology be used as a tool across all lines of business within an organization? How can IT better align with the organizational processes?

Resulting regulations have had far-reaching impacts on information technology—specifically controls and the auditing of those controls. These controls include general controls, which are embedded in IT services, as well as application controls, which are embedded in business applications. Why are these controls important? Why is the auditing of these controls important?

What If an Organization Does Not Comply with Compliance Laws?

Of course you wouldn't break a law, right? But asking what if your organization doesn't comply with compliance laws is a fair question. Let's look at an example of an individual compliance issue to understand why.

It is a law to come to a complete stop at a stop sign, yet many people ignore it. This scenario is actually a form of risk management. Many people consider it an acceptable risk to approach slowly and continue on if there is no traffic, without coming to a complete stop. The threat of another car exists, yet many people feel safe enough with the slow approach and rolling stop. There is always the threat of a police officer pulling you over and issuing a ticket. Yet how often is this enforced? If it were, what is the punishment? Given the likelihood of being pulled over by law enforcement, combined with what is likely a bearable fine, many people decide the risk is low and the benefit of noncompliance outweighs the risk.

NOTE

Don't forget about the other negative effects that noncompliance can have on an

organization, beyond the threat of fines and imprisonment. For example:

- Legal fees resulting from infringements contained within many regulations
- Brand damage and lost revenue as consumers abandon a business
- Negative effect upon stock price, hurting shareholder value
- Increases in the cost of capital

Organizations have spent and continue to spend large sums of money to achieve and maintain regulatory and industry compliance. This is especially true as regulations have placed greater accountability on individuals within an organization. Noncompliance can result in huge fines as well as jail time. Some regulations are subject to strict liability. Strict liability means even if there wasn't intent, government agencies can levy huge fines on organizations and some individuals can spend years in prison. Even greater punishments are in store where intent can be proven!

In addition to the financial and reputational consequences of noncompliance, organizations can also experience operational consequences. This can happen, for example, in the case of compliance standards imposed by the payment card industry. Potential consequences include payment card-imposed operational restrictions and even loss of card-processing privileges.

The **Payment Card Industry Data Security Standard (PCI DSS)** is an industry-created standard that applies to organizations that process credit cards. Companies that meet a specific threshold for large volumes of credit card transactions are required to achieve compliance. This is done via an audit by an independent Qualified Security Assessor (QSA).

Case Study: TJX Credit Card Breach

Imagine being the chief information officer (CIO) of one of the largest department store chains in the United States. Now imagine your CEO publicly announces that the company has just become the victim of the largest known theft of credit card data in history. This is a nightmare situation for any IT security professional, and this is what happened to The TJX Companies.

The TJX Companies, Incorporated is a large off-price retailer of apparel and home fashion. The company operates under several brands, including T.J. Maxx and Marshalls. On January 17, 2007, TJX announced it had become a victim of an intrusion into portions of its information systems that process and store customer transaction data.

An unauthorized intruder first accessed systems in July 2005, and unauthorized access continued through mid-January 2007. On December 18, 2006, TJX discovered suspicious software on its systems and immediately initiated an investigation along with leading computer security firms. Within a few days, TJX had notified law enforcement officials and met with the U.S. Department of Justice and the U.S. Secret Service to brief them on the discovery. Shortly thereafter, TJX notified contracting banks and payment card processing companies. Before the public announcement of the incident, the company had notified the U.S. Federal Trade Commission (FTC), the U.S. Securities and Exchange Commission (SEC), and the Canadian authorities.

At the time, this had evolved into the biggest credit card breach in history. Conservative estimates initially put the number at over 45 million credit and debit cards breached, as well as the personal information of hundreds of thousands of customers, including Social Security numbers and driver's license numbers.

NOTE

Initially, the TJX attackers accessed only historical data. To capture live transaction data, the attackers installed software that recorded the traffic. This enabled the attackers to steal credit card data as customer transactions were occurring in the store.

Although the exact details of the breach aren't clear, what is known is that the breach initially occurred as a result of the attackers targeting the wireless network of one of TJX's retail stores. The wireless network used Wired Equivalent Privacy (WEP) as an encryption method, which even at the time had been proven inadequate. The alternative was Wi-Fi Protected Access (WPA), which was introduced to replace WEP. Once the attackers penetrated this weak link, they eavesdropped on usernames and passwords used to log on to TJX's main systems in Framingham, Massachusetts. Eventually, the attackers created their own accounts on the main system and collected sensitive data.

In the aftermath, TJX has become the poster child for credit card breaches. The incident has also generated a lot of conversation and debate around adequate security controls for confidential personal information. Much of the blame for this incident was placed on the poorly secured wireless networks, but what type of defense in depth or compensating controls existed? The FTC charged TJX with failure to maintain proper security controls, specifically citing the lack of firewalls, wireless security, failure to patch vulnerabilities, and failure to update antivirus signatures.

The following are highlights of the fallout resulting from the breach. TJX:

- The company agreed to pay \$9.75 million to settle state investigations.
- The company settled with the FTC. As a result, TJX had to create a comprehensive security program to protect the confidentiality of personal information it collects. In addition, TJX must submit to a third-party audit of the program every two years for the next two decades.
- The company settled lawsuits brought by consumers and banker groups. Customers were provided with a special, three-day sale and vouchers as a result of the settlement of class-action lawsuits.
- The company settled with Visa and MasterCard for almost \$41 million.
- The company was required to implement a data-security program to ensure that this type of incident could never happen again.
- The company offered three years of credit monitoring to about 450,000 people who needed to provide their driver's licenses for transactions that occurred in the stores.
- The company set aside \$250 million for breach-related costs. Many analysts believe this number could ultimately be much higher.

NOTE

The TJX breach has since been eclipsed in size. Heartland Payment Systems announced a breach in 2009, which resulted in 130 million compromised payment card records. The attacker of Heartland Payment Systems was indicted in August of 2009, and was also the leader of the TJX breach.

Unlike the collapse of Enron and WorldCom, TJX did not break any laws. It was simply not compliant with stated payment card processing guidelines. Court documents filed by the banks that sued TJX indicated that TJX did not comply with 9 of the 12 broad provisions within the standard established for the payment card industry. Although the breach has

been costly for TJX, it is a multibillion dollar retailer that has survived and made appropriate adjustments. Smaller organizations, however, might not have survived.

Although it costs money to implement proper controls and procedures for compliance, noncompliance and security breaches have their own costs. You learned that fines can be levied for noncompliance, but what about the costs of a breach? Forrester Research puts the cost *per record* breached at anywhere between \$90 and \$305, depending on the type of breach and how regulated the industry within which the breach occurs is. Consider the following categories from where costs can occur following a breach:

- **Discovery, notification, and response**—Legal counsel, mailings, call center support, discounted product offers
- **Lost productivity**—Employees' attention diverted or put on other tasks requiring attention
- **Opportunity cost**—Loss of customers and attaining new customers
- **Regulatory fines**—FTC, PCI, Sarbanes-Oxley
- **Restitution**—Money set aside for payment
- **Additional security and audit requirements**—Those levied as a result of a breach
- **Other liabilities**

The following are some questions for further thought and discovery:

- Consider the reasons why TJX might have had the weaker WEP encryption configured. Was this the internal standard? Did retail equipment perhaps not support newer, more secure methods? If so, should compensating controls have been in place? What types?
- Do you feel that TJX properly handled the incident upon discovery of the breach? Consider how incident-response procedures are important to the IT security program.
- Had TJX collected and retained unnecessary personal data? What are the risks of holding onto data?
- Did TJX understand where customer data resided, how it was transmitted, and whether it was encrypted?
- If the data was encrypted, could the breach have been possible? Is it enough to just encrypt sensitive data? What about the cryptographic keys that perform the encryption/decryption of the data? How and where are those stored? Is this defined in a policy? If so, how is it audited?
- What were the results of TJX's payment-card processing audits and third-party vulnerability audits?
- Were weaknesses and vulnerabilities within TJX discovered and documented through internal security assessments?



CHAPTER SUMMARY

Conducting audits and assessments of IT environments has increasingly become more important and visible since the collapse of companies such as Enron and WorldCom in the early to mid-2000s. Although they might share similar qualities, the differences between an audit and an assessment can be great. Likewise, internal auditors and external auditors have many of the same functions, yet some important differences in their roles

and expectations. Regardless, assessments, audits, and auditors are all key components to ensuring a successful risk-management and compliance strategy. Adequate governance and oversight of these activities helps ensure that businesses don't follow the path that Enron and WorldCom did, and also helps in preventing incidents such as what TJX went through.



KEY CONCEPTS AND TERMS

Assurance

Audit

Compliance

Control Objectives for Information and Related Technology (COBIT)

Controls

Enron

Governance

National Institute of Standards and Technology (NIST)

Objectives

Payment Card Industry Data Security Standard (PCI DSS)

Penetration test

Risk

Risk management

Sarbanes-Oxley Act

The TJX Companies, Incorporated

WorldCom



CHAPTER 1 ASSESSMENT

1. A security assessment is a method for proving the strength of security systems.
 - A. True
 - B. False
2. Categorizing information and information systems and then selecting and implementing appropriate security controls is part of a _____.
3. Whereas only qualified auditors perform security audits, anyone may do security assessments.
 - A. True
 - B. False
4. NIST 800-53A provides _____.
5. Which one of the following is *not* a method used for conducting an assessment of security controls?
 - A. Examine
 - B. Interview
 - C. Test
 - D. Remediate
6. Which of the following is an assessment method that attempts to bypass controls and gain access to a specific system by simulating the actions of a would-be attacker?

- A. Policy review
 - B. Penetration test
 - C. Standards review
 - D. Controls audit
 - E. Vulnerability scan
- 7.** An IT security audit is an _____ assessment of an organization's internal policies, controls, and activities.
- 8.** Which of the following best describes an audit used to determine if a Fortune 500 health care company is adhering to Sarbanes-Oxley and HIPAA regulations?
- A. IT audit
 - B. Operational audit
 - C. Compliance audit
 - D. Financial audit
 - E. Investigative audit
- 9.** The internal audit function may be outsourced to an external consulting firm.
- A. True
 - B. False
- 10.** Compliance initiatives typically are efforts around all except which one of the following?
- A. To adhere to internal policies and standards
 - B. To adhere to regulatory requirements
 - C. To adhere to industry standards and best practices
 - D. To adhere to an auditor's recommendation
- 11.** At all levels of an organization, compliance is closely related to which of the following?
- A. Governance
 - B. Risk management
 - C. Government
 - D. Risk assessment
 - E. Both A and B
 - F. Both C and D
- 12.** Which one of the following is true with regard to audits and assessments?
- A. Assessments typically result in a pass or fail grade, whereas audits result in a list of recommendations to improve controls.
 - B. Assessments are attributive and audits are not.
 - C. An audit is typically a precursor to an assessment.
 - D. An audit may be conducted independently of an organization, whereas internal IT staff always conducts an IT security assessment.
 - E. Audits can result in blame being placed upon an individual.
- 13.** Noncompliance with regulatory standards may result in which of the following?
- A. Brand damage
 - B. Fines
 - C. Imprisonment
 - D. All of the above
 - E. B and C only
- 14.** Which of the following companies engaged in fraudulent activity and subsequently filed for bankruptcy?
- A. WorldCom
 - B. Enron
 - C. TJX

D. All of the above

E. A and B only

- 15.** Some regulations are subject to _____, which means even if there wasn't intent of noncompliance, an organization can still incur large fines.

CHAPTER 2

Overview of U.S. Compliance Laws

T

O STAY COMPLIANT WITH REGULATIONS first means you must interpret the regulation.

You must understand the gap between the regulation and your organization. The next step is coming up with a plan. Finally, you must execute the plan and implement measures to report compliance.

Without compliance laws and industry regulations, compliance means adhering to an organization's internal policies. However, it is likely that, whatever your industry, compliance laws exist to which you must adhere.

Many industry standards and government regulations affect IT operations. Remember, each country has its own laws and regulations. Thus, the number of compliance laws and regulations expands greatly. In this chapter, you will learn about many of the major regulations. Keep in mind that you are only scratching the surface. Other compliance regulations exist and are often specific to a particular industry.

Chapter 2 Topics

This chapter covers the following topics and concepts:

- What public and private sector regulatory requirements are
- What the Federal Information Security Management Act is
- What the U.S. Department of Defense requirements are
- What the Sarbanes-Oxley Act is
- What the Gramm-Leach-Bliley Act is
- What the Health Insurance Portability and Accountability Act is
- What the Children's Internet Protection Act is
- What the Children's Online Privacy Protection Act is
- What the Family Educational Rights and Privacy Act is
- What the Payment Card Industry Data Security Standard is
- What the Red Flags Rule is

Chapter 2 Goals

When you complete this chapter, you will be able to:

- Describe the goals and requirements for key acts of Congress
- Understand Department of Defense requirements and the importance of cybersecurity
- Describe the goals and requirements of the Payment Card Industry Data Security Standard

- Describe various regulations concerning protection of health, accounting, and other information

Introduction to Public and Private Sector Regulatory Requirements

Dealing with regulatory requirements is a hard task for many organizations. Troubles come from two directions. First, information technology personnel rarely have a legal background. Second, most requirements lack technical depth. This is because people drafting the regulations lack the information technology background. Many regulations are vague in their requirements. Therefore, proper technologies, depth of controls, and control frameworks become an important tool.

⚠ WARNING

There is an irony in regulatory compliance laws. Although the laws might appear complicated, they make high-level points that are simple to understand. A problem occurs when people interpret regulations in different ways.

Nevertheless, it is first important to understand why these requirements exist. In addition, you must have a broad understanding of which requirements exist. Regulatory requirements exist at different levels. Those levels include state, federal, and international. In addition, industry consortiums propose requirements. It is important to know which regulations apply to your organization. This helps you ensure you stay compliant and prevents you from trying to solve the same problem twice. In most cases, you should consult corporate counsel or legal to help identify which regulations apply.

technical TIP

Your internal policies should execute the regulatory policies with which you need to comply. Policies should follow a framework or complete structure. Having a framework demonstrates a company's planned approach. Meanwhile, the policies demonstrate a company's drive and support to be compliant. Take the time to properly build your internal policies. This rids you of many headaches in the event you must undergo an audit. In other words, ensuring your policies follow a solid framework to comply with different regulations really pays off.

⚠ WARNING

If you do business in other countries, you need to consider the requirements and compliance laws of those foreign countries. In addition, many U.S.-based companies rely on foreign, third-party service providers. This could result in noncompliance with U.S. regulations.

Aside from legal, there are many available sources for IT compliance requirements. These include, for example:

- Text of laws
- Administrative code
- External auditors

- Internal auditors
- Industry associations
- Third-party guidelines

Regulatory compliance is nothing new. However, government oversight and strong compliance regulations greatly increased in the early 2000s. This was mainly due to corporate scandals—Enron, WorldCom, and others. Consider how quickly the Web and other information technologies advanced. Then, the increased focus on IT and IT security becomes more apparent. Yet regulatory requirements and industry standards are not without their critics. Critics accuse requirements regulating publicly traded companies of putting U.S. corporations at a disadvantage. At the same time, they discourage listing on the U.S. stock exchanges. Further, critics describe laws regulating federal information systems as bureaucratic without helping security. Furthermore, consider the payment card standards. Critics call these standards unfair for small businesses and criticize the standards for failing to provide enough security.

Regulatory Acts of Congress

Congress enacts major legislation known as *statutes*. The president of the United States signs these **acts of Congress** into law. Examples of such acts include the E-Government Act of 2002, the Sarbanes-Oxley (SOX) Act, and the Health Insurance Portability and Accountability Act (HIPAA).

After such acts become law, various government agencies create and enforce the federal regulations authorized by those acts. Some examples of these government agencies are the Food and Drug Administration (FDA), Environmental Protection Agency (EPA), U.S. Securities and Exchange Commission (SEC), Federal Trade Commission (FTC), and Federal Communications Commission (FCC), to name a few. Congress first typically passes a statute to address a problem, such as a social or economic issue. These are considered enabling legislation. It allows **regulatory agencies** to create the necessary regulations to implement the law. (A regulatory agency is a public or government agency that has authority over some area of activity in a regulatory or supervisory capacity.) For example, the FCC creates regulations under the Children's Internet Protection Act (CIPA). The SEC creates regulations under the Sarbanes-Oxley Act.

Federal Information Security Management Act

The **Federal Information Security Management Act of 2002 (FISMA)** is contained within the E-Government Act of 2002, Public Law 107-347, as Title III. This act grants the importance of sound information security practices. It also controls the interest of national security and the economic well-being of the United States. This act was amended in 2014 by the Federal Information Security Modernization Act of 2014, which provides several key changes.

The purpose of FISMA is to do the following:

- Provide a framework for effective information security resources that support federal operations, data, and infrastructure.
- Accept the interconnectedness of IT. Ensure effective risk management is in place.
- Ensure coordination of information security efforts between civilian, national security, and law enforcement communities.
- Facilitate the development and ongoing monitoring of required minimum controls to protect federal information systems and data.
- Provide for increased oversight of federal agency information security programs.

- Recognize that information technology solutions may be acquired from commercial organizations. Leave the acquisition decisions to the individual agencies.

The need for FISMA evolved during the 1990s. Government agencies' IT systems became more like those of commercial organizations. They started to transition from traditional mainframe computing to internetworked systems. As the Web became commonplace, federal agencies started to develop their own Web sites and offer online services. There was a sudden awareness that systems were more open and vulnerable than before. This eventually got the attention of Congress.



WARNING

FISMA provides for what NIST cannot develop. NIST standards and guidelines apply to federal information systems. However, they do not apply to national security systems. According to FISMA, standards and guidelines for national security systems "shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President."

FISMA tasked the National Institute of Standards and Technology (NIST) to develop and set standards and guidelines. These apply only to federal information systems. Standards help categorize information and the systems. They are developed using a risk-based approach. They include the minimum information security controls. For example, standards include the management, operational, and technical controls to apply to information systems.

In support of FISMA, NIST developed the following publications:

- Federal Information Processing Standard (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"
- FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems"
- NIST Special Publication 800-18, "Guide for Developing Security Plans for Federal Information Systems"
- NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems"
- NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"
- NIST Special Publication 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View"
- NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems"
- NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems"
- NIST Special Publication 800-59, "Guideline for Identifying an Information System as a National Security System"
- NIST Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories"

To comply with FISMA, the appointed inspector general of the agency performs a separate, annual evaluation. The evaluation first tests the value of the IT security policies, procedures, and practices. A subset of the information systems within the particular agency is tested. If no

inspector general exists, an independent external auditor performs it. The external auditor submits the results to the Office of Management and Budget (OMB). The OMB is a cabinet-level office within the Executive Office of the President of the United States with oversight responsibilities. The OMB compiles the data from each agency. The OMB then prepares an annual report to Congress on compliance with the act.

At first, it appears only federal agencies need to worry about compliance, but this is not true. Federal agencies, for example, must care about their own systems as well as the systems of other contractors or organizations supporting the agencies. Any company or organization that expects to conduct business with the federal government needs to concern itself with FISMA.

TIP

The annual reports submitted to Congress from the OMB concerning FISMA compliance are publicly available online. You can find them at http://www.whitehouse.gov/omb/legislative_reports.

The changes signed into law in 2014 authorize the Secretary of the Department of Homeland Security (DHS) to assist the OMB. In addition, the changes affect reporting and notification requirements. Agencies are required to provide timely notification of major security incidents to the OMB. Agencies also are required to provide much more specific information related to threats and compliance.

U.S. Department of Defense Requirements

The United States Department of Defense (DoD) is a federal department. It is responsible for all agencies of the government relating to national security and the military. The DoD imposes many requirements on the management of their information systems. The same goes for organizations that work with, contract with, and provide services for the DoD. These requirements are within many federal laws and regulations. These laws span over a period of decades. Given the fast-paced changes around information technology, requirements have been rapidly evolving. This is especially true as systems have moved from traditional mainframe computing to more distributed and interconnected computing.

Information resource management (IRM) is the process of managing information resources to improve performance and accomplish the mission of defense agencies. The Paperwork Reduction Act of 1980 introduced IRM into law. This act provides the OMB with oversight concerning IRM. This oversight assumes that within the OMB's policies, individual agencies can maintain their own IRM.

In later years, various amendments strengthened the original implementation of the law. Most notably, agencies needed to develop processes to acquire, control, and assess information systems. In spite of these laws, the 1990s saw a large rise of distributed networking technology. This only created more IT management issues for the DoD.

In 1996, Senator William Cohen led further reform. The reform streamlined the process of acquisition of IT resources. The position of chief information officer (CIO) was formed within federal departments and agencies. This CIO position was previously the senior IRM official. Now the title was more like the civilian role and reported directly to the agency head. This gave it a more strategic focus with greater accountability to solve the IT problems plaguing the agencies.

There are many laws and regulations that apply to the DoD. These laws are both external and internal. They guide the operation, management, and protection of information systems.

Three key United States federal laws are as follows:

- The Paperwork Reduction Act of 1995
- The Clinger-Cohen Act of 1996
- The E-Government Act of 2002

The **Paperwork Reduction Act of 1995** furthers the goal of the original act (1980) to have federal agencies take more responsibility and be held more publicly accountable for reducing the paperwork they generate.

The **Clinger-Cohen Act of 1996**, formerly the Information Technology Management Reform Act, improves upon the acquisition, use, and disposal of federal IT resources. This act is the basis for designating the Chief Information Officer within the Department of Defense. The Act includes **10 U.S. Code Section 2223, Information Technology: Additional Responsibilities of Chief Information Officers** and **10 U.S. Code Section 2224, Defense Information Assurance Program**, which provide the basis for the following DoD directives:

- **DoD Directive 5144.01, Assistant Security of Defense for Networks and Information Integration/DoD Chief Information Officer—This assigns responsibilities, functions, relationships, and authorities to the DoD CIO.**
- **DoD Directive 8000.01, Management of the Department of Defense Information Enterprise**—This provides guidance for creating an “information advantage” for the DoD and those that support its mission.

The **E-Government Act of 2002** improves the management of electronic government services by establishing a framework that requires using the Internet and related technologies to improve citizen access to government information services. The act includes the following provisions:

- **Federal Information Security Management Act of 2002 (FISMA)**—This law establishes a framework for effective information security with regard to information resources that support federal operations.
- **OMB Circular, A-130, Management of Federal Information Resources**—This includes procedural guidelines for the management of federal information resources and how to fulfill the mandate set by FISMA.
- **OMB Circular A-11, Section 53, Information Technology and E-Government**—This allows the agencies and OMB to review and assess IT spending across the federal government to provide for more effective operations, including ensuring privacy and compliance with other acts.

Certification and Accreditation and Risk Management Framework

As part of FISMA, all federal systems and applications must adhere to well-known security requirements. These requirements are documented and authorized. This process has traditionally been known as **certification and accreditation (C&A)**. It is essentially a process of auditing systems before putting them in a production environment. The C&A process ensures that efforts are made to mitigate risks. Security controls on information systems must be properly implemented and maintained. It supports risk-management activities. In fact, the government has moved from its traditional C&A process, which relied on DoD-specific

methodologies, to a six-step **risk management framework (RMF)** developed by NIST as part of NIST Special Publication 800-37, “A Guide for Applying the Risk Management Framework to Federal Information Systems.” At a high level, this allows the government to conduct consistent and repeatable assessments of security controls. They also gain awareness of risks and allow authorized officials to more confidently accredit or validate a system on an ongoing basis.

Specifically, the RMF takes a less static approach over traditional C&A. RMF provides for better dynamic risk management, which is required in diverse and rapidly changing environments and threat landscapes. The RMF includes an emphasis on the following:

- Near real-time risk management
- Continuous monitoring
- Building information security into enterprise architecture planning and the system development lifecycle
- Aligning information systems security risk with the organization’s overall strategy
- Establishing responsibility and accountability for security controls

As part of a C&A or process of producing information for senior or authorizing officials about the state of information systems, the following are required:

- **System security plan**—The requirements, agreed security controls, and supporting documents. Examples are network diagrams, data flows, and risk assessment.
- **Security assessment report**—The evaluation results of security controls. This report might also include recommendations.
- **Plan of action and milestones**—The details mitigating controls. You may plan or apply controls to reduce vulnerabilities. You can also plan or apply measures to correct any deficiencies.



FIGURE 2-1 Six steps of RMF.

The six steps of the RMF are shown in [Figure 2-1](#) and include the following:

1. Categorizing the information system, giving consideration to the related data and the impact as a result of an incident
2. Selecting a baseline set of controls based on the previous categorization and supplementing the baseline as appropriate
3. Implementing and documenting the security controls
4. Assessing the security controls to ensure they are producing the desired results
5. Authorizing the operation of the information system based on an acceptable level of risk
6. Monitoring the security controls continuously

FYI

Before adoption of the RMF, the DoD Information Assurance Certification and Accreditation Process (DIACAP) and its predecessor, the DoD Information Technology System Certification and Accreditation Process (DITSCAP), were other methodologies for evaluating and accrediting information systems with the Department of Defense.

Cybersecurity

Cybersecurity is the practice of protecting computers and electronic communication systems as well as the associated information. Department of Defense Instruction 8500.1 establishes cybersecurity policy and assigns responsibilities under Section 2224 of title 10 USC. The DoD cybersecurity program operates through defense in depth and integrating personnel, operations, and technology. This includes all DoD-owned and DoD-controlled information systems that use DoD information. The Department of Defense cybersecurity program outlines the controls that protect and defend information and information systems by ensuring **confidentiality, integrity, and availability**. It also provides authentication and nonrepudiation.

Protecting confidentiality, integrity, and availability are common security objectives for information systems. This forms the foundation for cybersecurity.

- **Confidentiality**—Ensuring that information is not disclosed to unauthorized sources. Loss of confidentiality occurs when data is open to some unauthorized entity or process.
- **Integrity**—Ensuring the protection against unauthorized modification or destruction of data. Integrity also includes the quality of an information system regarding logical completeness and reliability of the hardware, software, and data structures.
- **Availability**—Ensuring timely and reliable access to data and services for authorized users.

NOTE

Confidentiality, integrity, and availability (C-I-A) are often referred to as the security triad, C-I-A triad, or A-I-C triad.

[Figure 2-2](#) shows these three security objectives as a protective triangle. If any side of the triangle fails, security fails. In other words, threats to the confidentiality, integrity, or availability represent risk.

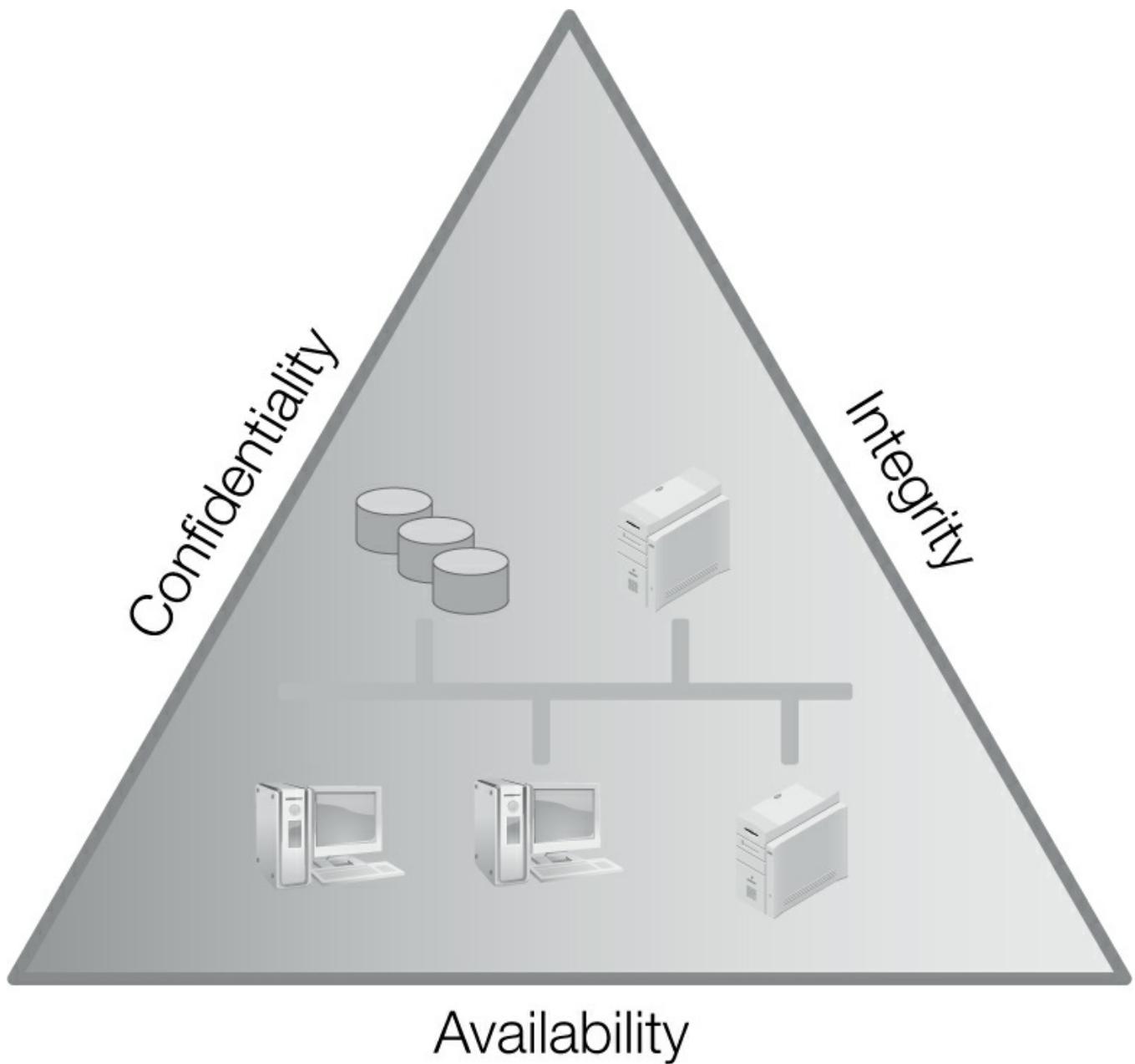


FIGURE 2-2 The C-I-A triad.

Information Assurance

Before the widespread use of the term *cybersecurity*, the DoD used the phrase *information assurance*. The concept has been around the DoD for many years and has evolved as information systems and the threats they face evolve. The Department of Defense originally set up information assurance from five pillars: assurance of confidentiality, integrity, availability, authentication, and nonrepudiation. One criticism might be that authentication and nonrepudiation are the only means of assuring the security triad. On the other hand, confidentiality, integrity, and availability are attributes of the information or information systems.

Regardless, these original five pillars are a key part of cybersecurity as defined by the DoD, which is, “prevention of damage to, protection of, and restoration of computers, electronic, communication systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”

In addition, the DoD considers authentication and nonrepudiation as two additional

measures. These two are joined with confidentiality, integrity, and availability. Authentication establishes the substance of a transmission, message, and originator. It also verifies an entity that has authorized access to information. Nonrepudiation provides assurance of proof of delivery and proof of identity. This way, neither party can later deny having processed or received the data.

Sarbanes-Oxley Act

The Sarbanes-Oxley Act of 2002, also known as Sarbox or SOX, is a U.S. federal law. It is the result of the Public Company Account Reform and Investor Protection Act and Corporate Accountability and Responsibility Act. Sarbanes-Oxley dramatically changed how public companies do business.

The bill stems from the fraud and accounting debacles at companies such as Enron and WorldCom. Former President Bush characterized the act “as the most far reaching reforms of American business practices since the time of Franklin Delano Roosevelt.” The act’s primary purpose was to restore public confidence in the financial reporting of publicly traded companies. As a result, the act mandated many reforms to enhance corporate responsibility, enhance financial disclosures, and prevent fraud. Sarbanes-Oxley consists of the following 11 titles:

- **Title I, Public Company Accounting Oversight Board (PCAOB)**—This establishes the Public Company Accounting Oversight Board (PCAOB). The PCAOB has several responsibilities, including overseeing public accounting firms, defining the process for compliance audits, and enforcing SOX compliance.
- **Title II, Auditor Independence**—This establishes the conditions of services an auditor can perform while remaining independent. For example, a public accounting firm that performs external auditing services cannot provide financial information systems design or internal audit outsourcing services.
- **Title III, Corporate Responsibility**—This requires the formation of audit committees. It also establishes the interactions between the committee and external auditors. Perhaps one of the more notable mandates of SOX is contained in Section 302, which requires the chief executive officer (CEO) and the chief financial officer (CFO) to take individual responsibility in certifying and approving the integrity of the company’s financial reports.
- **Title IV, Enhanced Financial Disclosures**—This addresses the accuracy and features of financial disclosures. For example, this title specifically addresses and prevents what Enron did, such as selling liabilities on its balance sheet as assets to special purpose entities (SPEs). This title also contains the controversial Section 404. Section 404 requires companies to report the adequacy of their internal controls.
- **Title V, Analyst Conflicts of Interest**—This fosters public confidence in securities research. This title defines code of conducts between firms.
- **Title VI, Commission Resources and Authority**—This provides greater authority to the SEC to fault or bar a securities professional from practice. This title also addresses the prevention of fraud schemes involving low-volume, low-price stocks.
- **Title VII, Studies and Reports**—This requires the comptroller general and the SEC to conduct studies and report their findings. Examples include studying the effects of the consolidation of public accounting firms as well as studying previous corporate fraud and accounting scandals.

- **Title VIII, Corporate and Criminal Fraud Accountability**—This provides the ramifications for corporate fraud and addresses the destruction of corporate audit records. This is a direct response to the auditing firm, Arthur Andersen, which shredded documents.
- **Title IX, White Collar Crime Penalty Enhancement**—This reviews the rules and penalties regarding white-collar criminal offenses.
- **Title X, Corporate Tax Returns**—This simply states that the CEO should sign the company tax return.
- **Title XI, Corporate Fraud Accountability**—Also known as the Corporate Fraud Accountability Act of 2002, this title provides additional guidelines regarding consequences of corporate fraud. It also provides the SEC with the authority to freeze the funds of companies suspected of violating laws.

Sarbanes-Oxley is quite large and contains many reforms to rally public confidence. It also improves corporate accountability and helps to avoid corporate fraud and dishonesty. Two sections receive much of the attention, especially of IT. The first is Section 302, “Corporate Responsibility for Financial Reports.” The second is Section 404, “Management Assessment of Internal Controls.” These two sections place vast constraints on IT security. Although neither section mentions IT or IT security, financial accounting systems rely heavily on IT infrastructure. Thus, it has strongly driven the subject of IT security into the boardroom.

Section 302 requires the CEO and CFO to personally certify the truthfulness and accuracy of financial reports. They start and make internal controls. Then, they must assess and report upon the internal controls around financial reporting every quarter. Section 404 goes a step further. Section 404 requires the company to provide proof. Again, they must assess the effectiveness of their internal controls, which a public accounting firm must audit and attest. They then publish this information in the company’s annual report.

SOX is lengthy and is specific in many areas—for example, criminal penalties for noncompliance. It still is very high level and leaves a lot of room for interpretation, especially concerning IT controls. SOX does not directly address IT control requirements. As a result, you need to become familiar with a couple of publications. These include the auditing standards created by the PCAOB and the SEC’s release on management guidance—17 CFR Part 241. In this codification, the SEC issued further interpretation and guidance regarding Section 404. It provides “an approach by which management can conduct a top-down, risk-based evaluation of internal control over financial reporting.” PCAOB also made a formal process to further define the criteria within Section 404. This process became Auditing Standard No. 2. This standard is now superseded by Auditing Standard No. 5, “An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements.” Some notable changes to provide greater clarity and a more prescriptive approach include the following four areas:

- Aligning Auditing Standard No. 5 with the SEC’s management guidance, mostly with regard to prescriptive requirements and definitions
- Adjusting the audit to account for the particular circumstances regarding the different size and complexities of companies
- Encouraging auditors to use professional judgment, particularly in using a risk-assessment methodology
- Following a principles-based approach to determining when and to what extent the auditor can use the work of others to obtain evidence about the design and effectiveness of the control

The standard also states that the auditor should use the “same suitable, recognized control framework” as the management of the company they are auditing. Furthermore, it even goes as far to suggest a suitable framework. That framework is the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

Gramm-Leach-Bliley Act

Also known as the Financial Modernization Act of 1999, the **Gramm-Leach-Bliley Act (GLBA)** repeals parts of the Glass-Steagall Act from 1933. The Glass-Steagall Act prohibited banks from offering investment, commercial banking, and insurance services all under a single umbrella. GLBA deregulates the split of commercial and investment banking. GLBA also provides provisions for compliance within Sections 501 and 521 to protect the financial information held by the industry. This protection is on behalf of the consumers. GLBA generally applies to financial institutions or any organization “significantly engaged” in financial activities. Examples include banks and securities firms. More examples are firms dealing with mortgages, insurance, tax preparation, debt collection, and much more. The FTC maintains and enforces GLBA.

To protect personally identifiable information (PII), GLBA divides privacy requirements into three principal parts:

- **Financial Privacy Rule**—The Financial Privacy Rule governs the collection and disclosure of customers’ personal financial information.
- **Safeguards Rule**—The Safeguards Rule requires financial institutions to develop, maintain, and implement policies. These policies should tell how they will protect customer information.
- **Pretexting provisions**—The Pretexting provisions protect consumers. This protection is from both individuals and organizations that obtain personal financial information under false pretenses.

Pretexting

Pretexting is a method of social engineering. It is more about human interaction than about technology. For success, you must manipulate others to divulge sensitive information. The root of pretexting is pretext, or a situation or reason that is deceptive or false. For example, investigators often use pretexting—at least in the movies! It typically involves some type of con or clever ruse.

Consider, for example, how to guess a password. You might use some programmatic mechanism to guess a password. Now consider how much easier it is to ask someone for the password, presumably under a pretext. This is one example of why companies so often reiterate that they will never ask you for your password. A famous recent example involved Hewlett-Packard (HP). At the time, contracted private investigators determined the source of an information leak. To do so, the investigators operated under a pretext. They impersonated HP board members or journalists from popular news outlets to obtain phone records.

There are countless examples of why pretexting occurs. The GLBA Pretexting provision protects consumers from evildoers trying to obtain personal financial information under false pretenses. Identity theft is the greatest risk to consumers should their information be compromised.

The Financial Privacy Rule requires financial institutions to provide notices to their customers. The notices explain their privacy policies, specifically covering the information collection and sharing practices of the company. The consumer is also given control over

limiting the sharing of their information or opting out. If the financial institution changes its policy, it must provide another notice to the consumer.

The Safeguards Rule requires financial institutions to develop an information security policy to consider the nature and sensitivity of the information they handle. The plan must include and the company must comply with the following:

- Designate at least one employee to coordinate an information security program.
- Assess the risks to customer information within each pertinent area of the company's operation. Evaluate the effectiveness of the current safeguards and risk controls.
- Implement a safeguard program. Regularly monitor and test it.
- Choose service providers that can maintain appropriate safeguards, and govern their handling of customer information.
- Evaluate and adjust the security program in view of events and changes in the firm's operations.

Likely, most organizations will protect against pretexting as part of their information security program. The best defense against pretexting is not technical, but rather awareness and training. Training is for both employees and customers. The Pretexting provision makes it illegal to do the following:

- Make a false, fictitious, or fraudulent statement or representation to obtain customer information from the financial institution or from its customers.
- Use forged, counterfeit, lost, or stolen documents to obtain customer information from the financial institution or from its customers.

Health Insurance Portability and Accountability Act

U.S. Congress enacted the **Health Insurance Portability and Accountability Act (HIPAA)** in 1996. The primary purpose of the statute is twofold. First, it helps citizens maintain their health insurance coverage. Second, it improves efficiency and effectiveness of the American health care system. It does so by combating waste, fraud, and abuse in both health insurance and the delivery of health care. The U.S. Department of Health and Human Services (HHS) is responsible for publishing requirements and for enforcing HIPAA laws. However, the Office of Civil Rights, a subagency of HHS, administers and enforces the Privacy Rule and Security Rule of HIPAA. These laws are divided across five titles, which include the following:

⚠️ WARNING

Hippo has the letter P in it twice—not HIPAA. Surprisingly, many vendors that sell HIPAA solutions and even the government are guilty of misspelling the acronym for the legislation in printed literature and on Web sites.

- Title I, Health Care Access, Portability, and Renewability
- Title II, Preventing Health Care Fraud and Abuse, Administrative Simplification; Medical Liability Reform
- Title III, Tax-Related Health Provisions
- Title IV, Application and Enforcement of Group Health Plan Requirements

- Title V, Revenue Offsets

Much of the focus around HIPAA is within the first two titles. Title I offers protection of health insurance coverage without regard to pre-existing conditions to those, for example, who lose or change their jobs. Title II provides requirements for the privacy and security of health information. This is often referred to as Administrative Simplification. The broader law calls for the following:

- Standardization of electronic data—patient, administrative, and financial—as well as the use of unique health identifiers
- Security standards and controls to protect the confidentiality and integrity of individually identifiable health information

As a result, the HHS has provided five rules regarding Title II of HIPAA. These include the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, the Unique Identifiers Rule, and the Enforcement Rule. These five rules affect information technology operations within organizations. Specifically, the Privacy Rule and Security Rule affect information security. HIPAA is primarily concerned with **protected health information (PHI)**. PHI is individually identifiable health information. PHI relates to physical or mental health of an individual. It can also relate to the delivery of health care to an individual as well as payment for the delivery of health care.

The Privacy Rule went into effect in 2003. It regulates the use and disclosure of PHI by covered entities. Covered entities, for example, include health care providers, health plans, and health care clearinghouses. In many ways, the Privacy Rule drives the Security Rule. Under the law, covered entities are obligated to do the following:

- Provide information to patients about their privacy rights and how the information can be used.
- Adopt clear privacy procedures.
- Train employees on privacy procedures.
- Designate someone to be responsible for overseeing that privacy procedures are adopted and followed.

The Security Rule followed the Privacy Rule. Unlike the Privacy Rule, however, the Security Rule applies just to electronic PHI (ePHI). The Security Rule provides for the confidentiality, integrity, and availability of ePHI, and contains three broad safeguards:

- Administrative safeguards
- Technical safeguards
- Physical safeguards

Each of the preceding safeguards consists of various standards. All are required or addressable. Required rules must be implemented, but addressable standards provide flexibility. This way, an organization can decide how to reasonably and appropriately meet the standard. Bear in mind, however, that addressable does not mean optional.

Administrative safeguards primarily consist of policies and procedures. They govern the security measures used to protect ePHI. [Table 2-1](#) provides a summary of the administrative safeguards, including the required and addressable standards.

TABLE 2-1 HIPAA administrative safeguards and implementation specifications.

SAFEGUARD	IMPLEMENTATION SPECIFICATION	REQUIRED/ADDRESSABLE
Security management process	Risk analysis Risk management Sanction policy Information system activity review	Required Required Required Required
Assigned security responsibility	Not applicable	Required
Workforce security	Authorization and/or supervision Workforce clearance procedure Termination procedures	Addressable Addressable Addressable
Information access management	Isolating health care clearinghouse function Access authorization Access establishment and modification	Required Addressable Addressable
Security awareness and training	Security reminders Protection from malicious software Logon monitoring Password management	Addressable Addressable Addressable Addressable
Security incident procedures	Response and reporting	Required
Contingency plan	Data backup plan Disaster recovery plan Emergency mode operation plan Testing and revision procedures Applications and data criticality analysis	Required Required Required Addressable Addressable
Evaluation	Not applicable	Required
Business associate contracts and other arrangements	Written contract or other arrangement	Required

TABLE 2-2 HIPAA physical safeguards and implementation specifications.

SAFEGUARD	IMPLEMENTATION SPECIFICATION	REQUIRED/ADDRESSABLE
Facility access controls	Contingency operations Facility security plan Access control and validation procedures Maintenance records	Addressable Addressable Addressable Addressable
Workstation use	Not applicable	Required
Workstation security	Not applicable	Required
Device and media controls	Disposal Media reuse Accountability Data backup and storage	Required Required Addressable Addressable

Physical safeguards include the policies, procedures, and physical controls put in place. These controls and documentation protect the information systems and physical structures from unauthorized access. The same goes for natural disasters and other environmental hazards. The physical safeguards include the four standards shown in [Table 2-2](#), along with the implementation specifications.

Technical safeguards consist of the policies, procedures, and controls put in place. These safeguards protect ePHI and prevent unauthorized access. [Table 2-3](#) lists the five safeguards and corresponding implementation specifications.

TABLE 2-3 HIPAA technical safeguards and implementation specifications.

SAFEGUARD	IMPLEMENTATION SPECIFICATION	REQUIRED/ADDRESSABLE
Access control	Contingency operations Facility security plan Access control and validation procedures Maintenance records	Required Required Addressable Addressable
Audit controls	Not applicable	Required
Integrity	Mechanisms to authenticate ePHI	Addressable
Person or entity authentication	Not applicable	Required
Transmission security	Integrity controls Encryption	Addressable Addressable

Although covered entities must comply with the previously listed safeguards and implementation specifications, there isn't a safeguard listed that should surprise organizations. In fact, most of these safeguards are addressed through best practices for any sensitive information.

In 2006, the Final Rule for HIPAA was issued—the Enforcement Rule—and set the penalties to be levied as a result of HIPAA violations. The Enforcement Rule also established the procedures for investigations and hearings into noncompliance. The potential for increased enforcement of noncompliance to HIPAA was later introduced in 2009 when the **Health Information Technology for Economic and Clinical Health (HITECH) Act** was signed into law. HITECH was part of the American Recovery and Reinvestment Act (ARRA). In addition to laying the groundwork for increased enforcement, HITECH also adds requirements for a breach notification. The notification is what an organization puts in action should PHI become disclosed in a readable—that is, nonencrypted—format.

Children's Internet Protection Act

The **Children's Internet Protection Act (CIPA)** is a federal law introduced as part of a spending bill that passed Congress in 2000. The FCC maintains and enforces CIPA. This act addresses concerns about children's access to explicit content (such as pornography) online at schools and libraries by requiring the use of Internet filters as a condition of receiving federal funds. CIPA is a result of previous failed attempts at restricting indecent content. The Communications Decency Act and the Child Online Protection Act faced Supreme Court challenges over the United States First Amendment. The reason was the act violated the right of free speech contained within the Constitution.

CIPA does not provide for any additional funds for the purchase of mechanisms to protect children from explicit content. Instead, conditions are attached to grants and to the use of E-Rate discounts. *E-Rate* is a program that makes Internet access more affordable for schools and libraries.

CIPA requires schools and libraries to certify compliance to implement an Internet safety policy and "technology protection measures." This means having technology in place that blocks or filters Internet access that is either obscene, harmful to minors, or represents child pornography. This includes implementing a safety policy and controls that address the following:

- Access by minors to “inappropriate matter” on the Internet
- The safety and security of minors when using electronic communication such as e-mail, chat rooms, and instant messaging
- Unauthorized access and unlawful activities by minors
- Unauthorized disclosure, use, and dissemination of personal information regarding minors
- Measures restricting minors’ access to harmful materials

Before implementing the policy and controls, however, the law also requires schools or libraries to first provide public notice and to hold a public hearing to address the proposed Internet safety policy.

You might have noticed that the term *inappropriate matter* could be considered vague and controversial. As a result, the act is clear in stating that the government may not establish the criteria for making such a determination. The act states that the determination is made at the local level by the school board, local educational agency, or library.

Finally, schools and libraries must comply with one more step before they can receive the E-Rate. They must certify they have an Internet safety policy in place meeting the preceding requirements. Noncompliance with the law occurs if there is a failure to submit for certification. In this case, the institution will not be eligible for services at the discounted rate. In addition, failure to ensure the use of the computers in accordance with a certification will be required to reimburse all funds and discounts for the certification period.

Children’s Online Privacy Protection Act

Like CIPA, the **Children’s Online Privacy Protection Act (COPPA)** is a United States federal law designed to protect children. COPPA is maintained and enforced by the FTC. COPPA requires Web sites and other online services aimed at children less than 13 years of age to comply with specific requirements of the law.

In 2013, the FTC implemented new provisions, which provide additional protections to keep pace with the changes in technology. The FTC also introduced a six-step plan to understand if an organization is required to comply with COPPA, and if so, how to be compliant. The six steps are as follows:

1. Determine if your company is a Web site or online service that collects personal information from kids under 13.
2. Post a privacy policy that complies with COPPA.
3. Notify parents directly before collecting personal information from their kids.
4. Get parents’ verifiable consent before collecting information from their kids.
5. Honor parents’ ongoing rights with respect to information collected from their kids.
6. Implement exceptions to COPPA’s verifiable parental consent requirement.

With Step 1, an organization will likely need to consult the law and to understand precisely how terms are defined. For example, what does it mean to *collect*, or what exactly is considered *personal information*? Online services are obliged to comply with COPPA if asking for information that would even imply a child is less than 13 years of age—for example, “Do you now attend elementary school?”

After it is determined that COPPA applies, the next step requires creation of a privacy policy. COPPA requires that the privacy policy list all operators who are collecting

information. In addition, it must list an operator who will respond to any and all queries from parents. Next, the privacy policy must contain a complete description of the personal information that is collected and for what purposes. Finally, the policy must state the rights afforded to parents. For example, this must include a notice that parents have the right to review the information collected on their child and even provide direction that the collected data be deleted.

Except under limited classes of information, COPPA requires that parents be notified before data is collected from their children. The rule provides for very specific requirements that must be met with regard to such notice. Once notification requirements are met in Step 3, Step 4 requires verifiable consent. While the means of providing such consent is left up to the requesting organization, the rule does provide several examples of acceptable methods. One simple example is a signed consent form via fax, mail, or electronic scan. Another is entry of a credit or debit card number when coupled with a financial transaction.

The final two steps require continual obligations upon the entity complying with COPPA. With Step 5, parents may ask to review, revoke, or delete the child's information at any time. Such requests must be honored by the complying organization. At the same time, the organization must take necessary precautions, such as taking reasonable measures to ensure that parents are in fact who they say they are. The final step provides rules around the need to protect the confidentiality and integrity of the information collected as well as ensure that adequate retention and disposal practices are maintained.

Family Educational Rights and Privacy Act

The **Family Educational Rights and Privacy Act (FERPA)** of 1974 is a U.S. federal law. FERPA protects the privacy of student education records. It also provides parents certain access rights to the student's educational records. Parental access rights stop once the student enters post-secondary education or the student turns 18 years old. The regulation applies to educational institutions that receive federal funding from the U.S. Department of Education.

Educational agencies or institutions should notify parents or eligible students of their rights under the law annually. The notice includes the right to do the following:

- Review the student's educational records. Under most situations, the school is not required to provide copies. They may charge to provide copies.
- Seek correction or revision of the educational records if believed to be inaccurate or a violation of privacy. If the school doesn't make any amendments, a formal hearing may be requested. If the school still doesn't make any changes, the parent or eligible student may place a statement regarding the content in question.
- Consent to disclosure of educational records. Schools may disclose directory information. However, schools must give parents or eligible students opportunity to restrict disclosure of the information. Disclosure of educational records and nondirectory information without consent is provided under certain conditions of the law.
- File a complaint with the department regarding failure to comply with the act.

As the name implies, *directory information* is personal data that you can find in publicly available sources. For example, a publicly available source could be a phone book or yearbook. Such information is not considered a harmful invasion of privacy. Examples of directory information include the following:

- Name
- Address
- Telephone number
- Date and place of birth
- Honors and awards
- Dates of attendance

WARNING

You may never disclose Social Security numbers as directory information, under the FERPA regulations. You cannot even use the last four numbers of your Social Security number, which is common across other industries.

Nondirectory information, on the other hand, includes, for example, Social Security numbers and transcripts.

In 2008, two relevant documents were published. The first was “Joint Guidance on the Application of the Family Educational Rights.” The second was the “Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records.” Many schools and universities operate health clinics. Thus, it is important that educational and health records kept at health facilities on campus are only subject to FERPA and not HIPAA. If the institution is a post-secondary school that provides health care to nonstudents, the health information of the nonstudent patients is subject to HIPAA.

Compliance with the law is typically the responsibility of the registrar’s office, which in turn works with legal counsel. However, IT professionals should be involved in the process and understand FERPA to ensure compliance. The act was originally drafted in 1974, so distributed networked computer technology was not around yet. Therefore, interpretation of the law is sometimes needed. Recent changes do help accommodate this technical evolution. Consider that the real meaning of FERPA is access and confidentiality—access in that parents or eligible students must be permitted access to their records and confidentiality in that education records must be protected and not released without written consent. Then, consider the number of electronic records relating to students that are likely to be stored on file servers and within databases. It is more difficult because IT makes tasks so easy, such as submitting and retrieving grades electronically, obtaining Web-based financial aid, and registering for courses.

NOTE

In the past, FERPA did not allow student ID numbers to be disclosed as directory information because they are used to both identify and authenticate the student. If a student identifier is not used to access records or for authentication, such as a password, it may be treated as directory information.

Under the FERPA Final Rules issued in 2008, FERPA does address further requirements and guidelines around information systems. The changes also urge “educational agencies and institutions to utilize appropriate methods to protect education records, especially in electronic data systems.” The update also addresses several examples of data breaches and the unauthorized disclosure of information. It also expresses concerns that data may be

compromised as a result of failure to implement proper security controls. Yet the update does not dictate how to properly safeguard electronic records, but instead offers additional resources—for example, NIST—on how to protect the information.

FERPA now provides suggestions on what to do in the case of an inadvertent release of data on the Internet or other unauthorized disclosure. In case of unauthorized disclosure, FERPA doesn't require notification. That is, the school does not have to issue direct notices to the parents or students. However, it does require the school to maintain a record of the disclosure. FERPA advises that direct notification should occur if the unauthorized disclosure might lead to identity theft. Nevertheless, other laws might still require institutions to provide direct notification.

Payment Card Industry Data Security Standard

You may recall that TJX is a company that suffered a serious breach in which it had millions of credit card numbers stolen. TJX was not the first, however, nor is it the last. Individual credit card companies started formulating programs to prevent breaches from occurring. These programs ensured that merchants meet baseline security requirements for how they store, process, and transmit payment card data.

The five leading credit card companies—Visa, MasterCard, American Express, JCB, and Discover—came together and formed the **Payment Card Industry Security Standards Council (PCI SSC)** in 2004. To help organizations that process card payments prevent credit card fraud, PCI SSC created the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is a set of requirements that prescribe operational and technical controls to protect cardholder data.

Adhering to PCI DSS requires three ongoing steps:

- **Assess**—Identify cardholder data as well as all related IT infrastructure and processes. This involves making sure adequate controls are in place and testing for vulnerabilities.
- **Remediate**—Eliminate the storage of unnecessary data and fix discovered vulnerabilities.
- **Report**—Submit validation records and compliance reports.

FYI

Compliance with PCI DSS is required for merchants and credit card processors. However, the PCI Security Standards Council also provides guidance for software developers of payment application systems and for manufacturers of PIN transaction systems. PCI PIN Transaction (PTS) Security Requirements are geared to the management of the devices used to protect cardholder PINs. Payment Application Data Security Standard (PA-DSS) is for the software developers of payment applications.

PCI SSC manages the overall program. However, card vendors have their own programs for compliance and enforcement. Determination of requirements depends on the volume of card transactions that take place. Any organization, however, that holds, processes, or passes cardholder data must undergo annual assessment. The assessment is required regardless of amount. In general, organizations that process a smaller number of transactions might only need to complete a self-assessment questionnaire (SAQ). Organizations with high-volume transactions must meet other requirements, such as assessment by an independent firm. The

firm must be designated as a **Qualified Security Assessor (QSA)**. (A QSA is an organization qualified and authorized to perform PCI compliance assessment.) In addition, requirement 11.2 requires vulnerability scans. The scans are done quarterly and are performed by a PCI **Approved Scanning Vendor (ASV)**. (An ASV is a qualified and approved company able to perform PCI vulnerability scans and assessment.)

 **TIP**

PCI DSS, SAQ, QSA, and ASV are some good acronyms to become familiar with. A list of qualified QSAs and ASVs is located at the PCI SSC Web site at <http://www.pcisecuritystandards.org>. The Web site also has procedures on how to become an ASV or a QSA.

PCI DSS is unlike most regulatory laws in one way. It is very specific with regard to requirements and expectations. The requirements generally follow security best practices and use the 12 high-level requirements, aligned across six goals, as shown in **Table 2-4**. Each requirement listed in the table consists of various subrequirements. Also included are procedures for testing. These must be documented as either being in place or not in place.

Consider requirement 8, for example. It requires a unique ID to be assigned to each person with computer access. Within the security standard, this requirement actually consists of 21 subrequirements. Many of them are very specific. For example:

- Incorporate two-factor authentication for remote access.
- Set first-time passwords to a unique value and change immediately after first use.
- Remove or disable inactive accounts at least every 90 days.
- Require a minimum password length of at least seven characters.

TABLE 2-4 Goals and high-level requirements for PCI DSS.

GOALS	HIGH-LEVEL REQUIREMENTS
Build and maintain a secure network.	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data.	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program.	5. Use and regularly update antivirus software or programs. 6. Develop and maintain secure systems and applications.
Implement strong access control measures.	7. Restrict access to cardholder data on a need-to-know basis. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly monitor and test networks.	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an information security policy.	12. Maintain a policy that addresses information security for employees and contractors.

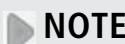
SSC should be read as qualified by the actual materials available from PCI SSC. For questions regarding PCI SSC, its programs or materials, please contact PCI SSC through its Web site at <https://www.pcisecuritystandards.org>.

Since PCI DSS started, the Security Council has released several supplemental documents, including the following:

- **Information Supplement: Requirement 11.3 Penetration Testing**—This provides clarification around penetration testing. It also discusses the difference from the PCI DSS-required vulnerability assessments.
- **Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified**—This recognizes the complexity and the possible unfeasibility of the original requirement. It provides further guidance regarding the intent and alternatives.
- **Navigating the PCI SSC—Understanding the Intent of the Requirements**—This provides further discussion regarding the purpose of each of the requirements.
- **Information Supplement: PCI DSS Wireless Guidelines**—This provides further guidance and suggestions for deploying 802.11 wireless local area networks (WLANs).

Red Flags Rule

Based on the Fair and Accurate Credit Transactions Act of 2003, the **Red Flags Rule** was created to establish a procedure for identifying possible instances of identity theft. The FTC along with the credit union and banking regulatory agencies created the Red Flags Rule. They are also responsible for enforcing it. The Red Flags Rule requires all financial institutions and creditors to implement an identity theft prevention program. The goal is to detect warning signs or red flags of identity theft.



The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace. In addition, it provides information to help consumers identify, prevent, and stop such activity.

The law applies to financial institutions such as banks, savings and loan associations, and credit unions. The law applies to any entity where a consumer has an account that conducts payments or transfers, such as a checking account. In addition, the law applies to creditors. Creditors extend, renew, or continue credit. Examples include finance companies, mortgage brokers, utility companies, and automobile dealers. For both financial institutions and creditors, the law applies only to covered accounts. Creditors use a covered account when there is a foreseeable risk of identity theft. A common example is an account used for household purposes. This includes such things as credit card accounts, mortgage loans, broker margin accounts, checking accounts, and so on.

To comply with the Red Flags Rule, financial institutions and creditors must follow four basic elements. These involve having appropriate policies and procedures in place to do the following:

- Identify red flags for covered accounts.
- Detect red flags.

- Respond to those red flags.
- Update the program periodically.

Financial institutions are first responsible for identifying red flags for covered accounts. The regulation does not demand specific red flags. Instead, it requires the financial institution or creditor to identify and create a list of red flags on its own. The regulation offers guidelines, however, in identifying red flags. [Table 2-5](#) lists the five categories provided by the regulation and includes an example of each.

After creating the list of relevant red flags, the institutions must then put programs and procedures in place to be able to detect the red flags. The regulation provides very little guidance on how to do this, other than saying what most institutions are already doing. For example, guidance might include getting unique information, verifying the person opening the account gives accurate and real information, and ensuring transactions are monitored. For many organizations, effective detection relies on technology solutions that specifically focus on authentication and fraud monitoring.

TABLE 2-5 Red flag categories and an example of each.

CATEGORY	EXAMPLE
Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services	A recent and significant increase in inquiry volume
The presentation of suspicious documents	A photograph or physical description on an identification not consistent with the applicant or consumer presenting the identification
The presentation of suspicious personal identifying information, such as a suspicious address change	A Social Security number (SSN) that has not been issued or is listed as the number of a deceased individual
The unusual use of or other suspicious activity related to a covered account	A notification to the financial institution or creditor that the customer isn't receiving paper account statements
Notice from customers, victims of identity theft, law enforcement, authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor	A notification from the customer to the financial institution or creditor of unusual activity

Next, the financial institutions and creditors must respond to the red flags. This prevents and lessens identification theft. Organizations must respond accordingly. For example, this ranges from contacting the customer to notifying law enforcement.

Finally, financial institutions and creditors should know that risks to customers and themselves are constantly changing. On one hand, business changes can affect risk tolerance. Examples include mergers and acquisitions as well as changes in the type of accounts offered to customers. On the other hand, methods of identity theft and how it's detected and prevented are constantly changing. A game of cat and mouse is the best way to describe the relationship among fraudsters, law enforcement, and vendors that provide prevention and detection tools.



CHAPTER SUMMARY

In addition to private industry standards, such as PCI DSS, companies must be concerned with and comply with many laws. Such requirements might affect only specific industries, whereas others can span across industries. PCI DSS, for example, generally affects any organization that holds, processes, or passes payment cardholder information, regardless of industry. HIPAA, on the other hand, primarily affects the health care industry, and Sarbanes-Oxley pertains to any publicly traded company.

Although compliance with regulations can touch many different groups within an organization, IT departments are increasingly discovering they need to stay abreast of the latest regulations as IT has become pervasive throughout organizations. It might seem overwhelming to keep up with the requirements of all the existing regulations, not to mention new ones. However, a sound governance, risk-management, and compliance program within organizations using a well-defined framework can make the process much more efficient and effective.



KEY CONCEPTS AND TERMS

10 U.S. Code Section 2223, Information Technology: Additional Responsibilities of Chief Information Officers

10 U.S. Code Section 2224, Defense Information Assurance Program

Acts of Congress

Approved Scanning Vendor (ASV)

Availability

Certification and accreditation (C&A)

Children's Internet Protection Act (CIPA)

Children's Online Privacy Protection Act (COPPA)

Clinger-Cohen Act of 1996

Confidentiality

Cybersecurity

E-Government Act of 2002

Family Educational Rights and Privacy Act (FERPA)

Federal Information Security Management Act of 2002 (FISMA)

Gramm-Leach-Bliley Act (GLBA)

Health Information Technology for Economic and Clinical Health (HITECH) Act

Health Insurance Portability and Accountability Act (HIPAA)

Information resource management (IRM)

Integrity

Paperwork Reduction Act of 1995

Payment Card Industry Security Standards Council (PCI SSC)

Pretexting

Protected health information (PHI)

Public Company Accounting Oversight Board (PCAOB)

Qualified Security Assessor (QSA)

Red Flags Rule

Regulatory agencies

Risk management framework (RMF)



CHAPTER 2 ASSESSMENT

1. Which of the following acknowledges the importance of sound information security practices and controls in the interest of national security?

 - A. FISMA
 - B. GLBA
 - C. HIPAA
 - D. FACTA
 - E. FERPA
2. What organization was tasked to develop standards to apply to federal information systems using a risk-based approach?

 - A. Public Entity Risk Institute
 - B. International Organization for Standardization
 - C. National Institute of Standards and Technology
 - D. International Standards Organization
 - E. American National Standards Institute
3. RMF provides for the authorization of the operation of an information system based on an acceptable level of _____.
4. Which of the following organizations was tasked to develop and prescribe standards and guidelines that apply to federal information systems?

 - A. NIST
 - B. FISMA
 - C. Congress
 - D. PCI SSC
 - E. U.S. Department of the Navy
5. What section of Sarbanes-Oxley requires management and the external auditor to report on the accuracy of internal controls over financial reporting?

 - A. Section 301
 - B. Section 404
 - C. Section 802
 - D. Section 1107
6. Sarbanes-Oxley explicitly addresses the IT security controls required to ensure accurate financial reporting.

 - A. True
 - B. False
7. Which of the following was established to have oversight of public accounting firms and is responsible for defining the process of SOX compliance audits?

 - A. COSO
 - B. Enron
 - C. PCAOB
 - D. Sarbanes-Oxley
 - E. None of the above
8. Which of the following is *not* one of the titles within Sarbanes-Oxley?

 - A. Corporate Responsibility
 - B. Enhanced Financial Disclosures
 - C. Analyst Conflicts of Interest
 - D. Studies and Reports

- E. Auditor Conflicts of Interest
- 9.** Which one of the following is *not* considered a principal part of the Gramm-Leach-Bliley Act?
- A. Financial Privacy Rule
 - B. Pretexting provisions
 - C. Safeguards Rule
 - D. Information Security Rule
- 10.** Which regulatory department is responsible for the enforcement of HIPAA laws?
- A. HHS
 - B. FDA
 - C. U.S Department of Agriculture
 - D. U.S. EPA
 - E. FTC
- 11.** Which one of the following is *not* one of the safeguards provided within the HIPAA Security Rule?
- A. Administrative
 - B. Operational
 - C. Technical
 - D. Physical
- 12.** In accordance with the Children's Internet Protection Act, who determines what is considered inappropriate material?
- A. FCC
 - B. U.S. Department of Education
 - C. The local communities
 - D. U.S. Department of the Interior Library
 - E. State governments
- 13.** While the Family Educational Rights and Privacy Act prohibits the use of Social Security numbers as directory information, the act does permit the use of the last four digits of a SSN.
- A. True
 - B. False
- 14.** PCI DSS is a legislative act enacted by Congress to ensure that merchants meet baseline security requirements for how they store, process, and transmit payment card data.
- A. True
 - B. False
- 15.** To comply with the Red Flags Rule, financial institutions and creditors must do which of the following?
- A. Identify red flags for covered accounts.
 - B. Detect red flags.
 - C. Respond to detected red flags.
 - D. Update the program periodically.
 - E. All of the above
 - F. Answers B and C only

CHAPTER 3

What Is the Scope of an IT Compliance Audit?

A

UDITS COME IN ALL SHAPES AND SIZES. Regardless of size, audits represent a

systematic and measurable assessment of the environment of an organization. Auditing for IT compliance is part of the ongoing process to ensure an organization is putting in place and maintaining effective security policies and controls. The audit makes use of various tools, but is primarily concerned with how the security policies are actually used. The IT environment is vast, and can be broken down into manageable and auditable chunks or domains. This chapter explores what is required to achieve and sustain compliance across different scopes of the IT environment.

Chapter 3 Topics

This chapter covers the following topics and concepts:

- What your organization must do to be in compliance
- What you are auditing within the IT infrastructure
- What your organization must do to maintain IT compliance

Chapter 3 Goals

When you complete this chapter, you will be able to:

- Understand what organizations need to do to achieve and maintain compliance
- Explain why protecting privacy data is important for achieving compliance
- Understand the process for selecting security controls
- Compare the different domains of IT infrastructure

What Must Your Organization Do to Be in Compliance?

Achieving compliance with external standards and regulations must be your first consideration in assembling a policy infrastructure. Being in compliance also means making sure the organization meets the expectations of the policy by enforcing the infrastructure put into place. Policy and, thus, compliance are not just about technical measures, however. They must also consider nontechnical methods. There is no definitive answer or solution an organization can purchase that will provide it with compliance. Each organization must determine what is appropriate for it. To do this, an organization must consider current laws and industry standards along with the organization's mission.

Organizational **policies** provide general statements that address the operational goals of an organization. The role of information technology is to help accelerate the business. At the same time, consider security and compliance with laws and regulations to safeguard data. Specifically, IT and IT security policies provide the same high-level directives. They are also concerned, however, with protecting the confidentiality, integrity, and availability of information and information systems. Specifically, this includes sensitive intellectual property of the organization and data that is commonly protected under privacy laws, such as personal information about individuals.

Complying with an organization's internal policy requires standards. Internal **standards** describe mandatory processes or objectives that align with the goal of the policies. Establishing both policies and standards is critical for ensuring the success of the organization as well as compliance with the myriad regulations with which organizations must comply.

A good starting place is with a solid organizational governance framework. This framework considers the applicable laws and regulations and then sets the high-level requirements to secure and control the IT infrastructure. Frameworks such as Control Objectives for Information and Related Technology (COBIT) provide a blueprint for implementing high-level controls within an organization. Further, control standards such as ISO/IEC 27002 and NIST 800-53 provide more specific security controls.

When policies and control framework are in place, organizations can start implementing specific controls. These additional controls can further address risks to the organization. Perhaps one of the greatest challenges is determining what specific controls to apply. Always consider what is reasonable and appropriate for your organization. Too often, organizations spend too much time and money implementing controls that go beyond the requirements. This can even have the negative result of impeding the mission of the organization. On the other hand, many organizations may get compliance tunnel vision. That is, they lose sight of really addressing risk, and are concerned only with being compliant.

Finally, consider that organizations are often required to comply with many different regulations. Many of these may have overlapping goals and intent. Therefore, you want to avoid chasing each one individually. By having sound policies in place and a framework for the application of controls, you will be able to map existing controls to each regulation, including future regulations. Thereafter, organizations perform a **gap analysis** to identify anything that is missing. A gap analysis is a comparison between the desired outcome and the actual outcome. From that gap analysis, the organization can address the gaps separately.



WARNING

If your organization uses penetration tests and vulnerability assessments to check technical compliance, be careful. These could have a negative effect on the systems (for example, bringing them down). Additionally, vulnerability and penetration tests are not a substitute for risk assessments.

Although compliance with internal policies and compliance with legal requirements should be closely tied together, each of these can be divided into two high-level control objectives. In fact, they are included as control objectives within ISO/IEC 27002. These include the following:

- Compliance with legal and regulatory requirements

- Compliance with security policies and standards and technical compliance

Compliance with legal requirements includes controls such as identifying all applicable legislation, respecting intellectual property rights (IPR), ensuring proper use of cryptographic controls, preventing misuse of information-processing facilities, and protecting organizational records as well as data and the privacy of personal information. Compliance with security policies and achieving technical compliance includes controls for complying with security policies and standards and for technical compliance audits.

Protecting and Securing Privacy Data

In general, it is understood that privacy data must be protected. What is not so clear, however, is what constitutes privacy data. Depending on the environment in which an organization operates, privacy can take on different meanings. The American Institute of Certified Public Accountants (AICPA) defines **privacy management** as “the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personal information.” Thus, privacy is about personal information that might be used to identify an individual. Examples include the following:

- Name
- Social Security number (SSN)
- Home address
- E-mail address
- Physical characteristics

Personal information can also be considered sensitive. Consider, for example, sensitive financial or health information. When combined with personal information, this information becomes personal *and* sensitive. As a result, the protection of this data becomes increasingly important when you consider the risks posed to this data, such as inadequate access controls, improper use, or unauthorized disclosure, to name a few.

For both individuals and organizations, the collection of personal data provides many benefits. Organizations, for example, benefit from increased market intelligence and competitive advantage, whereas individuals benefit from things such as personalized services and targeted offerings. On the other hand, individuals might be subject to spam and **identity theft** if that data is not protected properly. (Identity theft is the theft of someone’s personal information for unauthorized use.) The organizations also are subject to litigation, negative publicity, and even financial loss.

There are numerous methods used to protect privacy data. For example, organizations can do the following:

- Develop appropriate privacy policies.
- Establish the position of a **privacy officer**. This is a senior-level management position within an organization responsible for handling privacy laws and their impact on the organization.
- Conduct training and awareness around data handling, identity theft, and **social engineering**. Social engineering involves manipulating people into divulging information.
- Consider adequate controls around data retention and data destruction.
- Conduct regular risk assessments of access controls.

- Limit data to only that which is required.
- Consider security technologies such as encryption.

Privacy laws and regulations vary not just by industry, but also by areas in which business is conducted. In North America alone, there are many laws concerning privacy. Popular examples include the following:

 **TIP**

An auditor might want to conduct a social engineering assessment in which he or she impersonates an executive to obtain personal or sensitive data, simply by asking for it.

- **Health Insurance Portability and Accountability Act (HIPAA)**—The Privacy Rule within Title II of this act is concerned with the security and privacy of health data.
- **Gramm-Leach-Bliley Act (GLBA)**—The Financial Privacy Rule within the act is concerned with the collection and disclosure of personal financial information.
- **Children's Online Privacy Protection Act (COPPA)**—This act contains provisions for Web sites collecting personal information from children under 13 years of age.
- **National Do Not Call Registry**—This registry provides a choice for consumers as to whether they receive telemarketing calls at home.
- **SB1386**—The California Security Breach Information Act regulates the privacy of personal information.
- **Electronic Communications Privacy Act of 2000**—This act regulates and protects the privacy of e-mail and other electronic communications.
- **The Privacy Act of 1974**—This act imposes limits on personal information collected by U.S. federal agencies.
- **The Fair Credit Reporting Act (FCRA)**—This act regulates the use of consumer credit information.
- **Personal Information Protection and Electronic Documents Act (PIPEDA)**—This Canadian law addresses how organizations collect, use, and disclose of personal information.

As a result, IT compliance audits must consider privacy data and the application of an appropriate privacy control framework within organizations. First, consider the laws and regulations across multiple boundaries in which business is conducted. Further, the coordination between both general counsel and IT is necessary to understand both the legal and security repercussions.

Finally, organizations should consider a privacy audit. Most audits are concerned with the privacy oversight, privacy policies, and privacy controls within an organization. A privacy audit focuses on the following:

- Which privacy laws apply to the organization?
- Are the organizational responsibilities defined and assigned (for example, for the privacy officer and the legal department)?
- Are policies and procedures for creating, storing, and managing privacy data applied and followed?
- Are specific controls implemented, and are compliance tasks being followed? For

example, is privacy data encrypted? Are there privacy statements and an opt-out mechanism on the organization's Web site?

Designing and Implementing Proper Security Controls

Information security is largely about managing risk. That means IT controls are implemented depending on the risk they are designed to manage. Although the focus is on mitigating risk by implementing appropriate security controls, there are other ways to deal with risk. Risk can also be avoided, transferred, or accepted. For example, driving a vehicle poses many risks. Consider the risk of loss due to theft or an accident. Most people choose to transfer the risk by purchasing insurance. Others might accept the risk by not purchasing insurance. Still others might avoid the risk altogether by choosing not to drive.

Every day, you make personal decisions that consider controls in relation to risk. Being human naturally makes you vulnerable to many different threats, which can have a tremendous impact on you. Many people wear a seat belt while driving, for example, to mitigate the risk of an accident. Now think about how you might choose to protect your family while at home. Door locks are a good place to start. Door locks are also a relatively simple control. Yet some people have alarm systems, whereas others don't. The same concept applies to the threat of an assailant with a gun. Why doesn't everyone wear a bulletproof vest?

Managing risks involves making tradeoffs. A solid understanding of the risks and proper consideration of the tradeoffs results in the controls you select for your personal security and for the protection of information. It is necessary to properly assess and prioritize risk.

The process of selecting security controls needs to be part of an overall framework for risk management. For example, the following activities consider the implementation of controls within the context of such a framework:

NOTE

Assessing and prioritizing risk doesn't just provide security. It also prevents wasted time and money on unnecessary controls that might have a negative impact on the goals and missions of the organization.

- 1. Discover and classify data and information systems**—First, consider the confidentiality, integrity, and availability of the data and information systems. Next, examine the potential impact on the organization should confidentiality, integrity, or availability be compromised.
- 2. Select security controls**—After you consider the impact, select appropriate security controls based on the risk to the systems.
- 3. Implement security controls**—After selecting controls, put the controls in place to ensure risks are reduced to an appropriate level.
- 4. Assess security controls**—Perform an evaluation of the effectiveness of the controls. The assessment provides the necessary information to ensure they are implemented correctly and meeting the security requirements.
- 5. Authorize the controls**—After considering the system in relation to the assessment of the controls, determine whether the risk that remains, the residual risk, is at an acceptable level.
- 6. Monitor the controls**—Once controls are set, put a system of continuous monitoring in place. Changes within the organization or the information system, for example, might

result in the need to update the security controls. In addition, an event involving the identification of a new threat or an event resulting in a breach will require an immediate assessment and possibly a change to the applied security controls.

COBIT is a popular and widely used control framework for IT in general. A high-level control objective with COBIT as related to the IT process is to “ensure systems security.” This objective includes the following:

- Management of IT security
- Security plan
- Identity management
- User account management
- Security testing, surveillance, and monitoring
- Security incident definition
- Protection of security technology
- Cryptographic key management
- Malicious software, prevention, detection, and correction
- Network security
- Exchange of sensitive data

Although this framework provides a sound overall foundation of control objectives, other frameworks or standards provide guidance that is more detailed. Selecting security controls is best approached by first adhering to a common set of basic or baseline controls. Next, you might need to apply additional controls that are specific to the system or application. Finally, you might need to apply **compensating controls**. Compensating controls are necessary when a baseline security control cannot be implemented, for example.

Some common control baselines from the National Institute for Standards and Technology (NIST) are listed in Table 3-1. Controls described in the table are from NIST Standard 800-53. The controls are categorized by a high-level control family and include various controls that apply to each group. Within each family, the policy and procedures are always considered.

In another example, SANS (SysAdmin, Auditing, Network, Security) Institute created a list of 20 Critical Controls primarily addressing the technical control area. In 2013, SANS transferred responsibility for the controls, referred to now as the **Critical Security Controls**, to the Council on CyberSecurity, which is an independent, non-profit organization with a commitment to a secure and open Internet. Many people are more comfortable with the 20 Critical Security Controls than with other more comprehensive frameworks. This is largely by design. The intent of the list was to be “real world” and to provide actionable guidance that considers those controls that provide the largest security gains based on existing threats and vulnerabilities. The following list represents the 20 Critical Security Controls as of Version 5:

 **NOTE**

The 20 Critical Controls may frequently change based on the current environment. For the latest guidance, see <http://www.sans.org/critical-security-controls>.

1. Inventory of authorized and unauthorized devices

2. Inventory of authorized and unauthorized software
3. Secure configuration for hardware and software on mobile devices, laptops, workstations, and servers
4. Continuous vulnerability assessment and remediation
5. Malware defenses
6. Application software security
7. Wireless access control
8. Data recovery capability
9. Security skills assessment and appropriate training to fill gaps
10. Secure configurations for network devices such as firewalls, routers, and switches
11. Limitation and control of network ports, protocols, and services
12. Controlled use of administrative privileges
13. Boundary defense
14. Maintenance, monitoring, and analysis of audit logs
15. Controlled access based on the need to know
16. Account monitoring and control
17. Data protection
18. Incident response and management
19. Secure network engineering
20. Penetration test and red team exercises

TABLE 3-1 Family of security control baselines and corresponding examples.

CONTROLS FAMILY	CONTROL EXAMPLES
Access Control	Account Management; Separation of Duties; Least Privilege
Awareness and Training	Security Awareness; Security Training; Training Records
Audit and Accountability	Audit of Record Retention; Auditable Events
Security Assessment and Authorization	Plan of Action and Milestones; Security Authorization
Configuration Management	Baseline Configuration; Configuration Change Control
Contingency Planning	Contingency Training; Alternate Storage Site
Identification and Authentication	Identifier Management; Cryptographic Module Authentication
Incident Response	Incident Handling; Incident Monitoring; Incident Reporting
Maintenance	Controlled Maintenance; Maintenance Tools
Media Protection	Media Access; Media Marking; Media Storage
Physical and Environmental Protection	Physical Access Controls; Visitor Control; Fire Protection
Planning	System Security Plan; Privacy Impact Assessment
Personal Security	Personnel Screening; Personnel Termination
Risk Assessment	Security Categorization; Vulnerability Scanning
System and Services Acquisition	Allocation of Resources; Security Engineering Principles
System and Communications Protection	Denial of Service Protection; Boundary Protection
System and Information Integrity	Malicious Code Protection; Spam Protection; Error Handling
Program Management	Enterprise Architecture; Risk Management Strategy

Stop for a moment, review the 20 Critical Security Controls, and compare them with the

controls listed in [Table 3-1](#). How different are they? Is it possible to map many of the controls to controls of the other? Interestingly, the 20 Critical Security Controls map to about one-third of the NIST controls, with the goal of addressing the most critical based on an attack-based analysis. This basic control document was created based on the most prevalent types of attack. Again, these controls aren't meant to replace a more comprehensive set such as that provided by NIST. Rather, these 20 Critical Security Controls provide simpler "quick wins." [Table 3-2](#) contains a sampling of the first five types of attacks considered when developing the Critical Security Controls. Each attack type is followed by the most related Critical Security Controls. The complete list contains more than 23 attack types.

TABLE 3-2 Summary of attacks correlated to the Critical Security Controls.

ATTACK SUMMARY	CRITICAL SECURITY CONTROL
Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them.	1
Attackers distribute hostile content on Internet-accessible (and sometimes internal) Web sites that exploit unpatched and improperly secured client software running on victim machines.	2, 3
Attackers continually scan for vulnerable software and exploit it to gain control of target machines.	2, 4, 5
Attackers use infected or compromised machines to identify and exploit other vulnerable machines across an internal network.	2, 4, 10
Attackers exploit weak default configurations of systems that are more geared for ease of use than security.	3, 5, 10

What Are You Auditing Within the IT Infrastructure?

Across the infrastructure, an audit should focus primarily on the following three objectives:

- Examine the existence of relevant and appropriate security policies and procedures.
- Verify the existence of controls supporting the policies.
- Verify the effective implementation and ongoing monitoring of the controls.

Examining risk and IT controls throughout the IT infrastructure can be complex given the breadth of components across organizations. There are, however, a lot of similarities between different IT departments. It is helpful to define and, if necessary, break up the scope of the audit into manageable areas or domains of security responsibility. [Figure 3-1](#) illustrates these seven domains, which include the following:

- **User Domain**—The end users of the systems, including how they authenticate into the systems.
- **Workstation Domain**—The end users' operating environment.

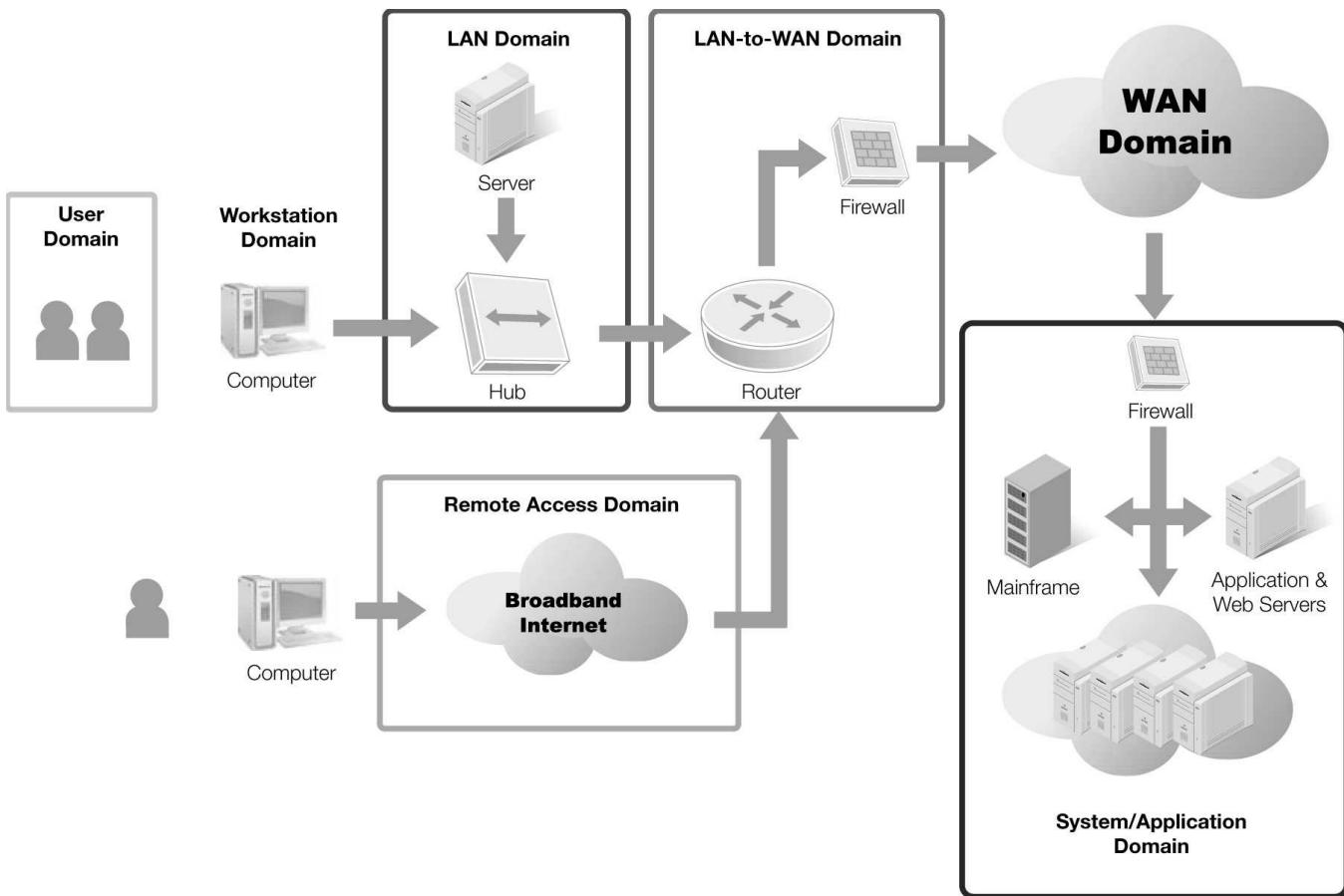


FIGURE 3-1 The seven domains of a typical IT infrastructure.

- **LAN Domain**—The equipment that makes up the **local area network (LAN)**. A LAN is a computer network for communications between systems covering a small physical area.
- **LAN-to-WAN Domain**—The bridge between the LAN and the **wide area network (WAN)**. A WAN is a network that covers a large area, often connecting multiple LANs.
- **WAN Domain**—The equipment and activities outside of the LAN and beyond the LAN-to-WAN Domain.
- **Remote Access Domain**—The access infrastructure for users accessing remote systems.
- **System/Application Domain**—Systems on the network that provide the applications and software for the users.

Within these seven domains, IT consists of hardware, software, network communications, protocols, applications, and data. Additionally, each domain is implemented within a physical space and includes people interacting with logical and physical aspects of the system. Breaking the audit into domains helps to define clear boundaries and determines the extent by which interconnected systems will be examined. An attacker needs to exploit a vulnerability in only one domain; however, each domain needs to be examined carefully. It only takes an exploit in one domain to weaken the others.

Although it is possible to separate these domains logically, there are many similarities concerning what is audited. For example, the following questions apply across these domains:

- Are there adequate policies and procedures in place?
- Are operating system security systems in accordance with standards and best

practices?

- Are auditing logs configured, and are they being reviewed?
- Are appropriate authentication mechanisms in place?
- Are access control lists (ACLs) in place and configured correctly?
- Are systems patched from known vulnerabilities?
- Are a disaster recovery plan and failover plan in place?
- What change control processes are in place, and are they followed?

This list represents only a small sample of questions to be asked and areas to be assessed. What is important to understand is that although each domain has its own unique characteristics, there are many overlapping requirements and controls.

User Domain

The **User Domain** covers the end users of information systems. An audit of the User Domain should be considered for anyone accessing the organization's information systems. This includes not just employees but nonemployees as well, such as contractors and consultants. This domain considers the roles and responsibilities of the users. It should examine all policies that relate to them—specifically, access policies.

The policies that apply might include the following:

- Acceptable use policy (AUP)
- System access policy
- Internet access policy
- E-mail policy

Additionally, the User Domain includes the method by which the user authenticates to resources. Depending on the organization's policy, users can authenticate in a number of ways. Regardless of the method used, the intent is to ensure that users are indeed who they claim to be.

NOTE

People are often the weakest link in IT security. You could have the strongest technical and physical controls, but if personnel don't understand the value of security, none of those controls will matter. Consider the simple example of users who write down their passwords. Often, users post these passwords right on the system itself. Users also visit risky Web sites and unknowingly download malicious software.

Workstation Domain

The **Workstation Domain** comprises the desktop environment of an end user's computing environment and includes the following:

- Desktop computers
- Laptop computers
- Printers
- Scanners

- Handheld computers and mobile devices
- Modems
- Wireless access points

Each of these devices should be authorized to access and connect to the organizational network and information resources. Thereafter, an audit of this domain would also ensure proper procedures and controls around maintaining the system hardware and software. Any desktop operating system, for example, should comply with the standards defined by the organization. The audit would take into consideration those security controls already applied. Standard operating systems and patch levels are typically mandated as well as specific configuration controls and the presence of anti-malware, desktop firewalls, and other security controls.

LAN Domain

A LAN is typically made up of computing and networking equipment in close proximity, such as a single room or building. LANs provide each computer on the network access to centralized resources, such as file servers and printers. In addition, they provide an easy method by which all the computers can be administered. Various other elements comprise the **LAN Domain**, including the physical connections required, such as the wiring, and networking equipment, such as hubs and switches. An audit of the LAN Domain can examine various elements, such as the following:

- Logon mechanisms and controls for access to the LAN
- Hardening and configuration of LAN systems
- Backup procedures for servers
- The power supply for the network

NOTE

Many organizations don't allow the use of hubs within a LAN. Although switches are more expensive, they provide greater benefits and increased security. However, an attacker can benefit greatly from an internal network port because few companies protect against rogue or unrecognized devices on their LAN.

Each individual device on the network must be protected or all devices can be at risk. A LAN is generally considered a trusted zone. Communications across a LAN are not usually protected as thoroughly as they might be if they were sent outside the LAN. A malicious person, for example, might be able to capture data going across the network quite easily. This is more easily done if hubs are used instead of switches. The attacker could simply plug into any network port in the building and capture valuable data. On the other hand, switches would require an attacker to have physical access to the switch. To prevent this, switches must be placed in secured rooms or secured closets.

LAN-to-WAN Domain

While a LAN typically covers a smaller defined geographical area, a WAN provides for long-distance communication to extend a network across a wider geographic area. Thus, a WAN can connect multiple LANs together. The transition from a LAN to a WAN typically involves

equipment such as a router or a firewall. A *router* is used to forward data between different networks. A *firewall* is another common component. A firewall is placed between networks and is designed to permit authorized access while blocking everything else.

The WAN Domain is considered an untrusted zone. It might be made up of components outside the direct control of the organization, and is often more accessible by attackers. The area between the trusted and untrusted zone, the **LAN-to-WAN Domain**, is protected with one or more firewalls. This is also called the boundary, or edge.

The public side of the boundary is often connected to the Internet and has public Internet Protocol (IP) addresses. These IP addresses are accessible from anywhere in the world. Attackers constantly probe public IP addresses looking for open ports and vulnerabilities. A high level of security is required to keep the LAN-to-WAN Domain secure.

An audit is critical to ensure that the environment is controlled correctly to prevent unauthorized access. There are many components and controls that work together to provide security. Organizations should carefully manage the configurations of all devices in this domain, such as firewalls, routers, and intrusion detection systems.

WAN Domain

The **WAN Domain** provides end-to-end connectivity between LANs. Like the LAN-to-WAN Domain, this environment includes routers, firewalls, and intrusion detection systems, but also has many more telecommunications components. Examples include channel service unit/data service unit (CSU/DSU), codecs, and backbone circuits.

For many businesses, the WAN is the Internet. A business may, however, lease semiprivate lines from telecommunications companies. These lines are semiprivate because they are rarely leased by only a single company. Instead, they are shared with other unknown companies. Again, the Internet is an untrusted zone. Any host on the Internet with a public IP address is at significant risk of attack, and you should expect any host on the Internet to be attacked even if that just means it is scanned for open ports and vulnerabilities. A significant amount of security is required to keep hosts in the WAN Domain safe. WAN audits help ensure the WAN is operating and configured as expected and is conforming to corresponding policies and standards.

Remote Access Domain

The **Remote Access Domain** is made up of the authorized users who access organization resources remotely. Access most often occurs over unsecured transports such as the Internet. Other unsecured transports include dial-up via a modem. Mobile workers often need access to the private LAN while traveling or working from home, for example. Mobile workers are granted this access using remote access solutions.

Remote access solutions, such as a virtual private network (VPN), can create an encrypted communications tunnel over a public network such as the Internet. Because the Internet is largely untrusted, remote access might represent a significant risk. Attackers can access unprotected connections. They might try to break into the remote access servers as well. Using a VPN is an example of a control to reduce the risk. VPNs, however, have their own vulnerabilities. For example, how does a user authenticate with the VPN? An attacker can gain access via the secured encrypted tunnel back to the corporate data just by knowing or guessing the credentials of the authorized user.

An audit should carefully consider the governing policies and procedures as well as the type of access provided.

technical TIP

A common control applied to VPN authentication requires the use of two-factor authentication. Two-factor authentication requires, for example, something the user knows and something the user has. This typically means a user is provided with a physical token that generates a new token code every minute. To authenticate, the user would provide his password or PIN as well as the token code. An ATM card used at an automatic teller machine to get cash uses a similar process. The user provides a PIN and inserts the card. The user requires possession of one item and knowledge of the other.

technical TIP

You should lock down or configure a server using the specific security requirements needed by the hosted application. Shutting down unnecessary services or software is a great first step in keeping a system secure. In addition, each application might require a new set of security measures or controls. An e-mail server requires one set of controls, whereas a database server requires a different set.

System/Application Domain

The **System/Application Domain** is made up of the many systems and software applications that users access. This, for example, includes mainframes, application servers, Web servers, proprietary software, and applications. Mail servers send and receive e-mail. Database servers host data that is accessed by users, applications, or other servers. Domain Name System (DNS) servers provide name-to-IP address resolution for clients. Knowledge within this domain can be very specialized. Operators may focus on one specific aspect, such as mail servers, and be quite familiar with associated security ramifications. On the other hand, that same person might know very little about databases.

Like the desktop operating system, server operating systems should be hardened to authorized baselines and configured according to policies and standards with the appropriate controls.

Maintaining IT Compliance

Simply achieving compliance is not enough. Compliance is an ongoing process that should be treated as a continuous function within the organization. Change is constantly occurring. The following are primary examples of why organizations must maintain IT compliance as an ongoing program:

- Organizations are dynamic, growing environments. As they adapt and grow, things change and compliance must be assessed against the changes.
- Threats evolve. Threats to organizations, like organizations themselves, constantly change and adapt. Organizations must respond and adjust appropriately to these threats.
- Laws, regulations, and industry standards continue to evolve, and new ones are introduced. Organizations are required to exercise due diligence. These efforts evolve as due care rises. What was good enough one day might not be enough the next.
- Many regulations require annual audits, ongoing reporting, and regular assessments against the environment.

Maintaining compliance requires a well-defined programmatic approach that involves processes and technology. This program needs to be monitored on an ongoing basis. At a minimum, the program should include the following:

- Regular assessment of selected security controls
- Configuration and control management processes
- Change management processes
- Annual audit of the security environment

Conducting Periodic Security Assessments

Regular security assessments should be part of the ongoing security strategy for any organization. Security assessments provide valuable metrics for maintaining compliance. In general, an assessment should address people, operations, applications, and the infrastructure throughout the organization. Because security assessments are conducted more often than, for example, an annual security audit, the purpose and the scope of a **risk assessment** can vary widely. Generally, a security assessment is grouped into different types:

- **High-level security assessment**—Provides an overall view of the information systems and is useful when examining across a broader scope
- **Comprehensive security assessment**—Provides a more targeted, concise, and technical review of information systems; involves control reviews and identification of vulnerabilities
- **Preproduction security assessment**—Used for new systems prior to being placed in production; may also be used for systems after having undergone a significant change

In addition to undergoing an initial security assessment, organizations should also determine how often they conduct assessments thereafter. Some of the considerations that should factor into the decision for ongoing assessments include the following:

- Expected benefits
- Scheduling requirements
- Applicable regulations and industry standards
- System and data classification

High-impact systems—for example, systems that process or store sensitive information—might require more frequent assessment than those that have a lesser impact. Also, consider when the last assessment was completed, as even a system with a moderate or low impact can present issues if the system has not been assessed in a long time. Often, the ongoing assessment process is driven by an organization's requirement to demonstrate compliance with regulations or standards.

Performing an Annual Security Compliance Audit

Regular security assessment should be supplemented with annual security audits. Although annual audits of specific functions are required for many organizations, an annual internal audit provides the organization with an independent review of the adequacy and effectiveness of IT security's internal controls. An audit should never be thought of as a one-time event.

In fact, as with security assessments, organizations have embraced the idea of continuous

auditing. An audit completed less than once a year can offer only a narrow scope of evaluation. This results in not providing real value for the organization. Organizations with an internal audit function are in the best position to implement audits that are more frequent or to put in place a continuous audit program.

Defining Proper Security Controls

The environments of controls are made up largely of a basic set of principles that apply across the various domains. These basic principles are embedded throughout security operations and administration management. These include the following:

- Defined roles and responsibilities
- Configuration and change management
- Environments for development test and production
- Segregation of duties
- Identity and authentication
- Principle of least privilege
- Monitoring, measuring, and reporting
- Appropriate documentation

When a basic control environment is in place, organizations can begin implementing additional controls to continue reducing risk to acceptable levels. An important aspect of maintaining compliance is defining and adjusting proper security controls. Although there are many different guiding documents for control standards, organizations must be careful of which specific controls they implement and how they put these controls into place.

Selecting and maintaining the right controls requires consideration of completed risk assessments. This risk assessment must address real threats while considering the tradeoff between risk and benefit. If you start by implementing controls properly along with proper documentation, then maintaining them shouldn't be as difficult. On the other hand, it might be easier to become complacent. As a result, organizations might not document the changes to controls and the implementation of new controls after a basic set is in place.

Creating an IT Security Policy Framework

IT security typically falls within an established IT policy framework. To maintain compliance, however, organizations should create a framework for IT security. A policy framework provides for a structured approach for outlining requirements that must be met. The framework can be thought of as a pyramid, as shown in [Figure 3-2](#).

The framework starts on the top with very clear and concise objectives or requirements, and then continues downward, exposing further details and additional guidance. At the topmost level is the policy. The policy regulates conduct through a general statement of beliefs, goals, and objectives. Next, standards support the policies. The standards are mandated activities or rules. Next, a **guideline** further supports the standard as well as the policy. Guidelines provide general statements of guidance, but are not mandatory. Here is an example of these three components:

- **Policy**—Users are required to use strong authentication when accessing company systems.
- **Standard**—Users are required to use two-factor authentication when accessing the remote network, combining a physical one-time token code with a personal

identification number.

- **Guideline**—Always keep your token within your possession and be aware of your surroundings when entering your personal identification number.

In addition to these three items, a **procedure** can also be part of the framework. A procedure provides step-by-step instructions that support the policy by outlining how the standards and guidelines are put into practice.

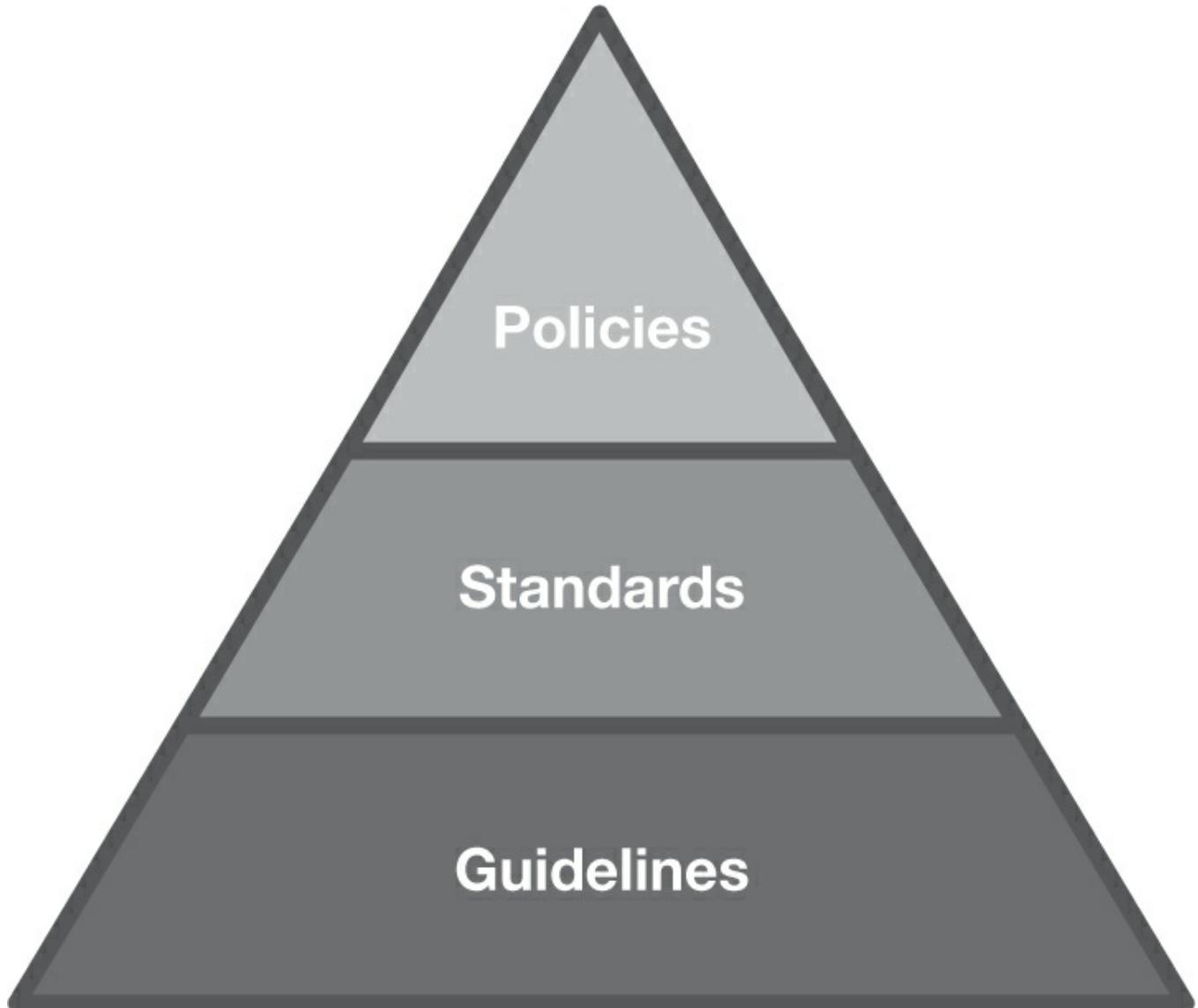


FIGURE 3-2 A policy framework.

Implementing Security Operations and Administration Management

Information technology has become a big part of the way in which organizations operate and enables customers, partners, and suppliers to stay connected. This requires the organization to implement and evolve its security and operations management functions to handle rapid change in accordance with stated policies. This added complexity makes it even more challenging to ensure that systems within the organization comply with security policies and standards. Consider that unauthorized changes are prevalent and new vulnerabilities appear daily. In addition, mistakes are bound to happen with the configuration and deployment of new systems. Auditing tools, industry standards, and frameworks provide solid foundations on which to base security operations and administration management.

Configuration and Change Management

Although **configuration and change management** isn't typically considered a function of IT security, it is very much related because of its implications with regard to IT security. Configuration and change management is a process of controlling systems throughout their life cycle to make sure they are operating as intended in accordance with security policies and standards. Additionally, configuration and change management involves the identification, control, logging, and auditing of all changes made across the infrastructure.

Configuration and change management is typically founded upon baseline configurations defined for systems. Subsequently, it ensures that authorized changes to the system do not affect their security. Additionally, change and configuration management provides a method for tracking unauthorized changes. Changes that are not authorized can negatively affect the system's security posture. Thus, a process for change and configuration management ensures that changes are requested, evaluated, and authorized. The following represents the high-level process:

1. **Identify and request change**—A need for a change is recognized and a formal request is submitted to a decision-making group.
2. **Evaluate change request**—An impact assessment is done to determine operational or security effects the change may have on the system or related systems.
3. **Decision response**—A decision typically results in the request either being approved or denied.
4. **Implement approved change**—If the request is approved, the change can be implemented in the production environment.
5. **Monitor change**—Administrators ensure the system operates as intended as a result of the change.

A review board usually manages this five-step process. A committee of employees from multiple disciplines within the organization makes up this board.



CHAPTER SUMMARY

While the law requires audits, organizations find it more necessary to conduct regular assessments. Regular assessments help ensure that audits will be more successful as well as ensure the confidentiality, integrity, and availability of information and information systems. The protection of privacy data needs to be considered in addition to just the protection of intellectual property. Audits and assessments usually begin based on a framework. When a foundation is in place, companies are finding it easier and more effective to conduct regular audits and assessments. Various frameworks from which to implement a risk management and policy program as well as frameworks that guide audits and assessments are discussed next. Understanding and managing the scope of a compliance audit are critical for efficient audits as well. Later in this book, you will learn more about achieving compliance within the seven domains of IT infrastructure.



KEY CONCEPTS AND TERMS

Compensating controls
Configuration and change management
Critical Security Controls
Gap analysis
Guideline
Identity theft
LAN Domain
LAN-to-WAN Domain
Local area network (LAN)
Policies
Privacy management
Privacy officer
Procedure
Remote Access Domain
Risk assessment
Social engineering
Standards
System/Application Domain
User Domain
WAN Domain
Wide area network (WAN)
Workstation Domain



CHAPTER 3 ASSESSMENT

1. After mapping existing controls to new regulations, an organization needs to conduct a _____ analysis.
2. Which of the following best describes the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personal information?
 - A. Security management
 - B. Compliance management
 - C. Privacy management
 - D. Personal management
 - E. Collection management
3. The process of selecting security controls is considered within the context of risk management.
 - A. True
 - B. False
4. If a baseline security control cannot be implemented, which of the following should be considered?
 - A. Compensating control
 - B. Baseline security standard revision
 - C. Policy revision
 - D. None of the above
5. Account management and separation of duties are examples of what type of controls?
 - A. Audit and accountability
 - B. Access control

- C. Security assessment and authorization
 - D. Personal security
- 6.** Which one of the following is *not* one of the seven domains of a typical IT infrastructure?
- A. User Domain
 - B. Workstation Domain
 - C. LAN-to-LAN Domain
 - D. WAN Domain
 - E. Remote Access Domain
- 7.** Which of the following policies would apply to the User Domain concerning the seven domains of a typical IT infrastructure?
- A. Acceptable use policy
 - B. Internet access policy
 - C. Security incident policy
 - D. Firewall policy
 - E. Answers A and B
 - F. Answers B and D
- 8.** Mitigating a risk from an IT security perspective is about eliminating the risk to zero.
- A. True
 - B. False
- 9.** Which of the following is an example of why an ongoing IT compliance program is important?
- A. Organizations are dynamic, growing environments.
 - B. Threats evolve.
 - C. Laws and regulations evolve.
 - D. All of the above
- 10.** Policies, standards, and guidelines are part of the policy _____.
- 11.** Which one of the following is *not* part of the change management process?
- A. Identify and request
 - B. Evaluate change request
 - C. Decision response
 - D. Implement unapproved change
 - E. Monitor change
- 12.** What can be done to manage risk? (Select three.)
- A. Accept
 - B. Transfer
 - C. Avoid
 - D. Migrate
- 13.** Regarding the seven domains of IT infrastructure, the Workstation Domain includes which of the following? (Select three.)
- A. Desktop computers
 - B. Laptop computers
 - C. Remote access systems
 - D. E-mail servers
 - E. Handheld devices
- 14.** Adequate controls over privacy data helps prevent _____ theft.

Auditing for Compliance: Frameworks, Tools, and Techniques

CHAPTER 4

Auditing Standards and Frameworks

CHAPTER 5

Planning an IT Infrastructure Audit for Compliance

CHAPTER 6

Conducting an IT Infrastructure Audit for Compliance

CHAPTER 7

Writing the IT Infrastructure Audit Report

CHAPTER 8

Compliance Within the User Domain

CHAPTER 9

Compliance Within the Workstation Domain

CHAPTER 10

Compliance Within the LAN Domain

CHAPTER 11

Compliance Within the LAN-to-WAN Domain

CHAPTER 12

Compliance Within the WAN Domain

CHAPTER 13

Compliance Within the Remote Access Domain

CHAPTER 14

Compliance Within the System/Application Domain

CHAPTER 4

Auditing Standards and Frameworks

C

ONDUCTING AUDITS AND ASSESSMENTS is challenging in the absence of a standard against which to audit or assess. Two concepts that are helpful include **control objectives** and **control activities**. Control objectives, despite the rapid evolution of technology, remain mostly constant. These tend to be high level and describe the goal for the organization. Control activities provide details on how to achieve the goals of the relevant control objective. There is no such thing as a one-size-fits-all framework or standard. Frameworks and standards simply provide the building blocks and guidance needed for organizations to tailor them to their specific needs. They are useful for guiding the control objectives and control activities. They are also useful for developing governance, risk management, and compliance. They provide auditors guidance from which to base their audit.

Organizations should create a methodology for governance, security, and compliance. Choosing from guiding control standards and frameworks is an ideal start. This chapter explores the importance of such standards and frameworks. This chapter also introduces several popular frameworks and standards in use today. There are still many more. Regardless, all have a common theme of putting in place sensible practices within organizations.

Chapter 4 Topics

This chapter covers the following topics and concepts:

- Why frameworks are important for compliance auditing
- Why standards are important in compliance auditing
- What ISO and IEC standards are
- What NIST 800-53 provides
- What the Cybersecurity Framework is
- How to develop a hybrid auditing framework or approach

Chapter 4 Goals

When you complete this chapter, you will be able to:

- Understand the importance of using a framework for audits
- Describe various strategies for using standards and frameworks for compliance auditing
- Understand COSO and how it relates to information technology
- Describe the key parts and importance of COBIT
- Understand the importance and benefits of an SOC engagement

- Describe the key ISO/IEC standards that relate to information security
- Describe the NIST 800-53 and 800-53A standards
- Understand the need for hybrid auditing approaches

Why Frameworks Are Important for Auditing

In general, a **framework** is a conceptual set of rules and ideas that provide structure to a complex and tough situation. Although a framework may be rigid in its skeleton, the idea is to provide flexibility. This chapter, for example, follows a framework to help guide the actual text and provide consistency. The framework includes distinct components, such as an introduction, learning objectives, headings, and a summary. Yet the authors have flexibility as long as they are within the confines of this framework.

Information technology (IT) environments are different from one to the next. Despite many similarities, each environment is different. Each company, for example, has different objectives. They have different ways of achieving goals. They have different risk profiles. IT departments exist to help support and drive the business. As long as no two organizations are exactly alike, neither will two IT departments be exactly alike.

An auditor must deal with multiple types of organizations. As a result, each audit is different. The size of the audit varies. The resources needed for the audit vary. The steps carried out for each audit also vary. A framework, however, provides a consistent system of controls to which IT departments can adhere. This system of controls also provides an auditor a consistent approach for conducting audits.

Controls tend to be either descriptive or prescriptive. A **descriptive control framework** provides for governance at a higher level. These control frameworks are important in helping to align IT with business or enterprise goals. The challenge is that they don't provide a prescribed method for turning these objectives into action. A **prescriptive control framework approach helps standardize IT operations and tasks, while still allowing for flexibility.** Organizations often apply both approaches together within IT, and audits tend to make use of both.

A more governing and descriptive type of framework may dictate a control objective that each IT organization should ensure systems security. Such an approach typically provides additional controls, such as ensuring network security or ensuring identity management. A major component of ensuring network security involves using firewalls. How each organization actually applies this varies. What if there is not a local area network-to-wide area network (LAN-to-WAN) connection? In this case, there may not be a firewall at any border; there may only be firewalls between internal network segments. One company might use a software firewall. Another might use hardware. There are also different types of firewalls. An administrator might use an Application Layer firewall in one situation and a Network Layer firewall in another. For the auditor, the control objective stays the same, yet the audit procedure may vary because of the differences.

NOTE

People often use the terms **framework** and **standard** interchangeably. Most frameworks are referred to as standards. Some standards, however, wouldn't necessarily be called frameworks—especially those that are very prescriptive. Often, you will hear these referred to as **best practices** or **good practices** as well.

The Importance of Using Standards in Compliance Auditing

There is no shortage of frameworks and standards for IT departments and auditors to rely on. There are many different standards from varying organizations, each with its own strengths and weaknesses. However, they all have the same common goal of establishing prudent and good practices around IT control. Many organizations find that they need to use a blend of standards to accomplish their goals. Auditors tend to focus or specialize on particular standards, yet many organizations may seek an audit or assessment against a particular standard. Many organizations, in the beginning, look to their peers and to auditors for what framework and standards they should be using. It is important, however, to consider the needs of the specific organization.

While trying to determine a specific standard to which to adhere, it is helpful to consider the high-level differences among them. Consider the following attributes that vary among different standards and frameworks:

- **Depth and breadth**—Some go far and wide, whereas others are narrow and deep. Guiding principles that cover a wide range might be most suitable to your organization. Alternatively, more prescriptive guidance around describing and assessing actual controls might be helpful.
- **Flexibility**—One standard might apply across the entire organization, whereas another might be limited to a specific department or team.
- **Reasoning**—Some standards provide stronger guidance about why they make a particular statement around controls. Sometimes, the reasoning can be important, as those putting in place and auditing controls understand how and why they apply.
- **Prioritization**—Although each organization determines acceptable risk, some standards can provide guidance for focusing on certain areas over others.
- **Industry acceptance**—Some standards are generally accepted more than others. Acceptance also varies by industry.

Standards and frameworks are closely tied to the previous discussion of policies and standards. A framework should offer IT organizations a method for establishing an approach to managing IT risks. The use of a framework combined with an analysis of risk helps guide the development of appropriate written policies and standards within the organization. A high-level control from a framework might state, for example, that systems should be protected from unauthorized access. As a result, an organization develops several policies that pertain to enforcing authorized access to its systems. One such policy states that individuals are assigned unique user names and passwords for the system. In turn, a standard may dictate specific parameters—for example, usernames must follow the format of first initial preceded by last name and be at least eight alphanumeric characters. Finally, a procedure indicates how to apply the requirements on a particular system.

Clear documented policies, standards, and procedures provide auditors with an obvious path upon which to base their audits. An unclearly documented policy structure makes the auditor's and auditee's jobs much more difficult. Audits go more smoothly when both parties work from closely aligned frameworks and accepted practices. If, for example, an auditor discovers a lack of clear policies, a standard provides a solid baseline on which to base the findings. For example, an audit deficiency that states that password security should "be stronger" is less powerful than one that states that password requirements aren't up to a specific standard or best practice.

Auditing against standards works best when the auditor and the organization agree on a

specific standard. Organizations first select frameworks most appropriate to their business. Then, it's the auditor's job to evaluate whether the company-selected standard is reasonable. The auditor must assess against the standard. This is one reason why most companies go with recognized and mature standards. The following are some key recommendations when selecting a standard:

- **Select a standard that can be followed**—This allows the standards to be more easily put in place. It also allows others within the organization and auditors to embrace the standards.
- **Employ the standard**—This reduces liability for having selected a specific standard that is not actually put into place.
- **Select a flexible standard**—This provides the organization the ability to remain responsive to changing business environments and consider its own risk profile.



WARNING

A standard control framework provides a strong foundation for an internal policy structure. However, failure to act on or meet what has been stated in an internal policy may result in an audit deficiency.

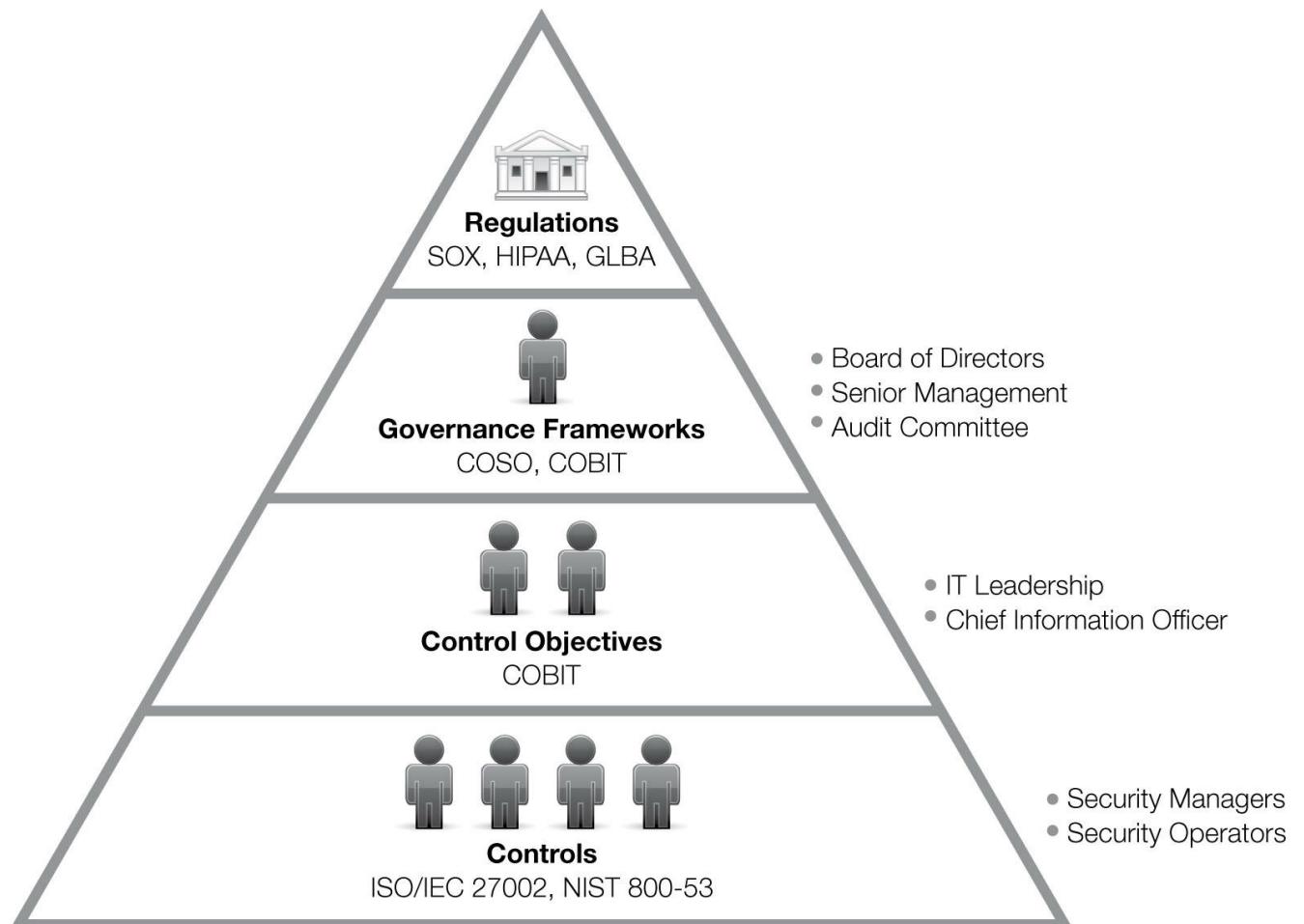


FIGURE 4-1 The hierarchy of standards and personnel.

In the next sections, you'll learn about different frameworks and standards. Standards are relevant to the individuals and groups within the organization. [Figure 4-1](#) illustrates the hierarchy of governance and controls. The diagram includes sample standards as well as the people to which they apply.

Following are the high-level steps an organization [may take to apply the use of standards:](#)

1. Educate personnel, beginning with senior management.
2. Choose the standards that the organization will follow.
3. Put the people in place and provide the needed resources to apply and meet the standard.
4. Confirm the standards are being met by using an internal audit and outside resources as needed.

COSO

The **Committee of Sponsoring Organizations (COSO) of the Treadway Commission** was founded in 1985 as part of a program to study the reasons that lead to fraud in financial reporting. Today, the mission of COSO is to “improve organizational performance and governance,” as well as “reduce the extent of fraud in organizations.” This is achieved through thoughtful leadership and frameworks, as well as guidance on the following:

- Risk management
- Internal controls

- Fraud deterrence

COSO issued a framework titled *Enterprise Risk Management—Integrated Framework*. This provides the structure to examine risk within the organization and apply risk-based processes.

The COSO **enterprise risk management (ERM) framework** consists of eight components across four objectives. The framework is geared to achieving an organization's objectives as defined by the following:

- **Strategic**—The high-level goals that support the overall mission of the group
- **Operations**—The effective and efficient use of the organization's resources
- **Reporting**—The reliability of reports
- **Compliance**—Adherence with applicable laws and regulations

Both reporting and compliance are within the control of the organization. ERM provides reasonable assurance of meeting these two objectives. On the other hand, strategic and operational objectives aren't always within the complete control of an organization. Both of these objectives are often influenced by external events. Thus, ERM can provide reasonable assurance that management is made aware in a timely manner of the degree to which the organization is moving toward achieving these two objectives.

The COSO framework identifies eight interrelated parts in connection with the management processes of an organization. These are as follows:

TIP

Many organizations choose COSO and see it as the only viable high-level, risk-management framework. The reason for this is that the Securities and Exchange Commission (SEC) recognizes COSO. It is specifically identified as a suitable framework within additional regulatory guidance around Sarbanes-Oxley compliance

- **Internal environment**—Establishing a culture in a company that tolerates or even favors risk
- **Objective setting**—Setting objectives, which is necessary to later establish how negative events might affect achieving those objectives
- **Event identification**—Identifying external events that might affect the organization's ability to achieve its objectives
- **Risk assessment**—Analyzing risk by considering the likelihood of adverse events and the impact they would have on the business
- **Risk response**—Considering the organization's appetite for risk as well as the response to take to risks, such as avoiding them or accepting them
- **Control activities**—Establishing policies and procedures to ensure that risk responses are carried out
- **Information and communication**—Identifying and communicating information in a timely manner so that people within the organization can perform their responsibilities
- **Monitoring**—Continuously monitoring and adjusting the ERM program as needed

The COSO framework is quite broad and applies across the functions of a company. Although

IT security is not specifically addressed, COSO addresses risk management across the organization. COSO does not describe any controls and is not prescriptive.

The framework is targeted at senior management and the board of directors. The chief information security officer (CISO) is likely to be involved in the risk-management process and in determining how controls are derived. IT departments should supplement COSO with a framework more specifically suited to IT. An excellent example is discussed next.

► NOTE

COSO was updated in 2004. The 2004 update introduced three new components. These included objective setting, event identification, and risk response. In October 2014, an announcement was made that the framework will again be updated from the 2004 version.

COBIT

Control Objectives for Information and Related Technology (COBIT) is an IT control framework originally published by the **Information Technology Governance Institute (ITGI)**, a think tank providing thought leadership on IT governance. ITGI published the COBIT framework in 1994 in cooperation with **ISACA**, a global professional organization that provides industry knowledge and good practices for information systems. COBIT offers an IT-specific framework, and is an excellent supplement to COSO. COBIT provides corporate management, IT management, and auditors with an accepted set of processes and controls to develop IT governance and control within an organization. Specifically, COBIT allows IT management to develop clear policies and apply good practices. COBIT even considers other standards as it seeks to be the overarching IT governance framework. COBIT is business-focused, process-oriented, controls-based, and measurement-driven. COBIT considers risk and stays close to the business by focusing on the benefits associated with IT. COBIT helps to align IT with the business or enterprise requirements by doing the following:

- Mapping controls to key business requirements
- Classifying IT activities into a process model
- Identifying the key IT resources to be controlled
- Defining the framework for control objectives

By providing enterprise-focused alignment, management is able to better understand what IT does. In addition, COBIT provides additional benefits:

- Clear accountability and responsibility
- Acceptance from third parties, auditors, and regulators
- Fulfillment of COSO requirements with regard to the IT control environment

What Is ISACA?

ISACA was once an acronym for Information Systems Audit and Control Association. Today, ISACA goes only by the acronym in an effort to appeal to a broader range of groups. In the late 1960s, ISACA was formed by a group of like-minded individuals seeking guidance on the auditing of computer systems. This group initially became known as the EDP Auditors Association.

Today, ISACA has more than 200 membership chapters in more than 80 countries, with more than 115,000 members. ISACA is behind several globally recognized professional certifications for information

systems auditors and IT security and governance professionals. ISACA also publishes a technical journal and hosts conferences worldwide. ISACA, along with its affiliated IT Governance Institute, provides several valuable resources to IT professionals. In addition to COBIT, the following frameworks are also available from ISACA:

- **Information Technology Assurance Framework (ITAF)—A framework for IT** assurance, the **Information Technology Assurance Framework (ITAF)** is applicable to any formal audit or assessment.
- **Risk IT Framework**—A framework based on guiding principles, the **Risk IT Framework** provides the structure to identify, govern, and manage IT risk.
- **Val IT Framework**—A framework that governs IT investments, the **Val IT Framework** helps businesses get more value out of their IT assets.
- **Business Model for Information Security (BMIS)**—This model helps to further align IT security with the business by providing a common language and business-oriented approach to managing information security.

These frameworks were also intended to complement COBIT. In fact, in COBIT 5, the current version of COBIT, they are actually covered within the scope of the COBIT framework.

ISACA also publishes additional standards, guidelines, procedures, and research for information system auditors and IT professionals. For students, ISACA offers a student membership program geared to those considering a career in IT.

COBIT serves as a valuable framework across different groups. For example, management can use COBIT to assess the performance of IT processes by comparing enterprise goals against the IT-related goals. Both types of goals are provided within COBIT. Those implementing COBIT as well as auditors can leverage the control requirements and assigned responsibilities from within COBIT.

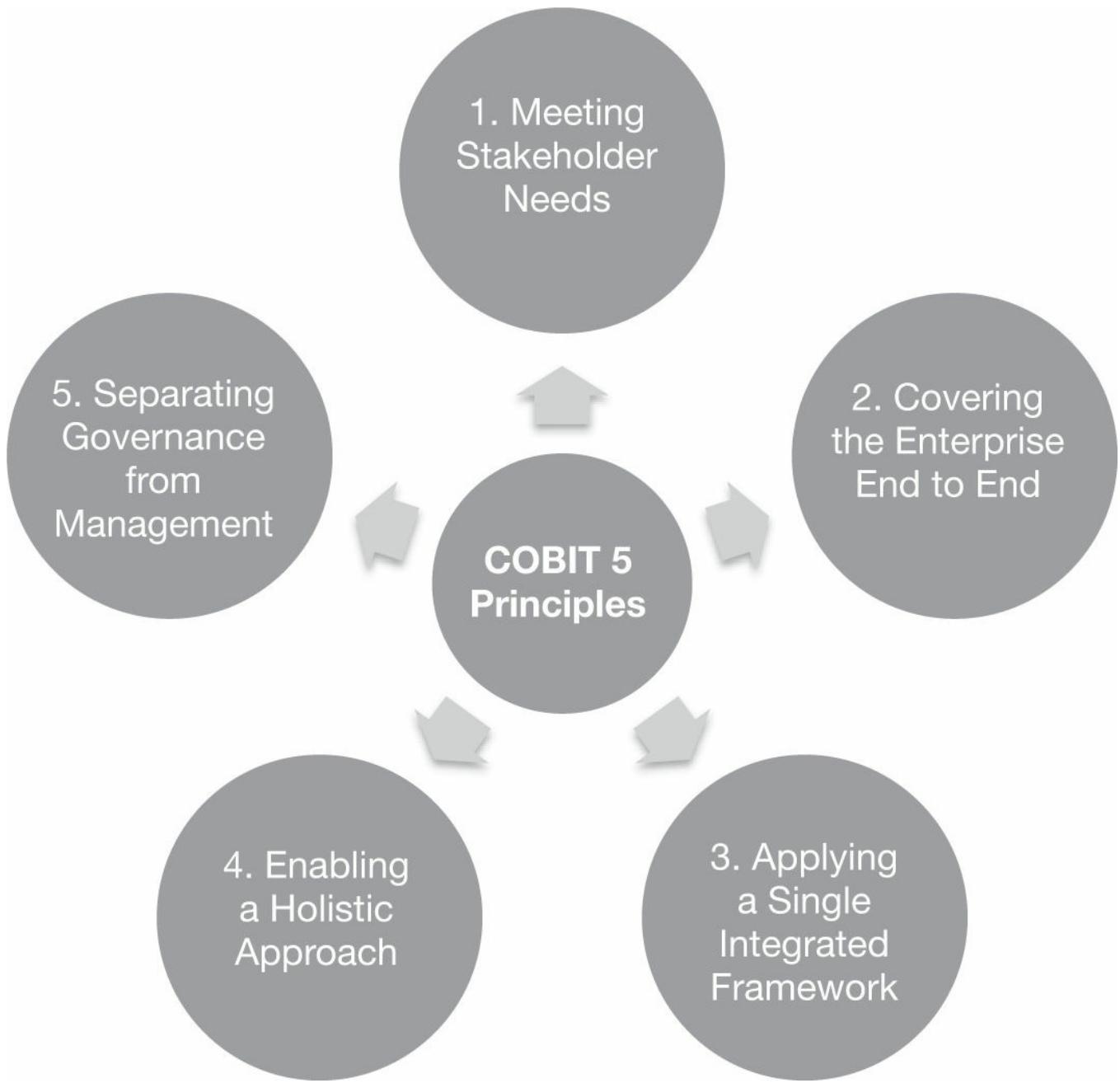


FIGURE 4-2 The COBIT 5 principles.

The current version of COBIT is COBIT 5. The COBIT 5 framework is based on the five principles shown in [Figure 4-2](#). According to the ISACA Web site:

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

Before looking at the framework in depth, let's first explore some of the major components of IT governance. The IT Governance Institute, which was formed by ISACA, defines five areas of IT governance. Before COBIT 5, these areas were explicitly called into focus within COBIT.

These areas are now currently built throughout the various processes. These areas of IT governance include the following:

- **Strategic alignment**—Ensures IT is aligned with the business
- **Value delivery**—Enables IT to deliver benefits to the business
- **Resource management**—Ensures the proper management of IT resources and that they are used responsibly
- **Risk management**—Involves being aware of risks and the organization's tolerance for risk
- **Performance measurement**—Tracks and monitors the application of IT processes from the strategic level to individual projects

Let's take a deeper look at COBIT 5 through the five principles.

Meeting Stakeholder Needs

The first principle, "Meeting Stakeholder Needs," largely addresses two important ideas:

- An enterprise exists to create value for the stakeholders. Stakeholders can vary widely by organization. In one simple example, customers and shareholders are examples of external stakeholders of a publicly traded company. Internally, a stakeholder can be any employee up to a board member.
- Value that is created must be done so in a way that also considers risk and the appropriate use of resources. Therefore, it is important that the enterprise be aligned properly to IT resources.

To help with this alignment, COBIT 5 introduces a goals cascade. This in essence states that the needs of stakeholders are influenced by a number of different drivers. These needs are broadly defined in the following three categories:

- Benefits realization
- Risk optimization
- Resource optimization

Based on the needs, you can then do a map to enterprise goals to determine which goals are primary or secondary. COBIT 5 provides 17 sample goals across the following four dimensions:

- Financial
- Customer
- Internal
- Learning and growth

For example, the following are the five sample enterprise goals in the internal dimension:

- Optimization of business process functionality
- Optimization of business process costs
- Managed business change programs
- Operational and staff productivity
- Compliance with internal policies

Next, COBIT 5 defines the 17 IT-related goals. To achieve enterprise goals, multiple IT goals are typically aligned with the enterprise goals. Again using the internal dimension, the following are seven IT-related goals:

- IT agility
- Security of information, processing infrastructure, and applications
- Optimization of IT assets, resources, and capabilities
- Enablement and support of business processes by integrating applications and technology into business processes
- Delivery of programs delivering benefits on time, on budget, and meeting requirements and quality standards
- Availability of reliable and useful information for decision making
- IT compliance with internal policies

Finally, these IT-related goals cascade down to what are known as *enabler goals*. Enablers are things such as processes or people. The enablers influence the outcomes and help accomplish goals.

Covering the Enterprise End to End

Principle 2, “Covering the Enterprise End to End,” is a foundational concept within COBIT 5. This principle includes both the governance and management of information and technology. The governance system first begins with an objective. Recall from the first principle that creating value as an objective is defined across three categories of needs. Taken together, these interact with the rest of the system through three other elements, which include the following:

- **Governance enablers**—This includes resources such as people and other resources like frameworks and processes.
- **Governance scope**—While the scope for COBIT 5 considers the entire enterprise, the scope can also take on smaller views.
- **Roles, activities, and relationships**—This provides definitions for those involved. This element answers the who, what, and how as related to those involved.

Applying a Single Integrated Framework

The third principle, “Applying a Single Integrated Framework,” is an important concept for COBIT 5, and one that makes it significantly different from previous versions of COBIT. For example, the contents of the COBIT 5 knowledge base are made up of several components. This includes the COBIT 5 enablers, which are unique to COBIT, but also factors previously outside COBIT. Examples include the following:

- ISACA guidance previously published separately, such as Val IT, Risk IT, and BMIS
- New ISACA guidance materials
- Other standards and frameworks, such as ISO standards

From this collective framework, content filters can now be applied to provide for varying degrees of guidance. For example, this includes specific COBIT 5 enabling or professional guides. For the latter, this could include COBIT 5 as related to information security only.

Enabling a Holistic Approach

Principle 4, “Enabling a Holistic Approach,” is all about enablers. Recall that enablers influence the outcomes and help accomplish the goals that drive them. COBIT 5 defines the following seven categories of enablers:

- Principles, policies, and frameworks
- Processes
- Organizational structures
- Culture, ethics, and behavior
- Information
- Services, infrastructure, and applications
- People, skills, and competencies

To provide for a structured way to deal with enablers and to manage the interactions and ultimately facilitate a successful outcome, COBIT 5 defines four dimensions. That is, each enabler has the following:

- Stakeholders
- Goals
- Lifecycle
- Good practices

Finally, a performance-management component is baked into this. Based on metrics, this determines if using the enablers is having a positive outcome.

Separating Governance from Management

The final principle to cover is the fifth principle, “Separating Governance from Management.” COBIT 5 makes a strong statement on the differences between governance and management. This is because they differ greatly and each ultimately serve a different purpose. According to COBIT 5, governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

On the other hand, “management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.” For each of the enabling categories described previously, COBIT 5 provides the model for the interaction required between governance and management.

So this model divides governance and management into their own domains. The governance domain consists of several processes in which the practices of evaluate, direct, and monitor (EDM) are defined. The management domain is divided into four domains or responsibility areas—plan, build, run, and monitor—from which 32 specific management processes are defined.

Plenty of resources are available to enable and implement COBIT 5 and these five principles. These include, for example, ISACA’s *COBIT 5 Implementation* professional guide.

Service Organization Control Reports

These days, most organizations outsource some function of their infrastructure to a third-party business. Imagine you are the owner of a company. Deciding to put your company’s

sensitive data in someone else's hands is a difficult decision to make. You'll likely want to ensure that certain controls are in place before you take on such a risk. The functions provided by the third-party businesses are going to affect the user organization's records. This could be your customer's health or financial information, for example.

As a result, service organizations find it important to instill trust and confidence in their customers. The service organization has a vested interest in helping its customers understand that adequate controls and processes are in place. **Service Organization Control (SOC) reports** provide such assurance. The Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) issues and maintains these auditing standards. The primary stakeholders for SOC reports include the following:

- **User entities**—The user entities, or organizations that rely on a service provider, benefit from SOC reports because they mitigate the risk associated with outsourcing services.
- **Service organizations**—The service organizations want to earn and keep the business of the user entities. SOC reports provide user entities with confidence and the assurance of trust.
- **Auditors**—Auditors from both the service-organization side and the user-entity side must understand the framework and standards for performing SOC engagements.

The **Sarbanes-Oxley Act (SOX)** has placed increased importance on SOC assessments. A goal of SOX is to maintain investor and public confidence through the accuracy and reliability of financial reporting. SOX essentially mandates the establishing of adequate internal controls. Consider that many organizations outsource all sorts of activities that could have implications on SOX. These include payroll functions, for example, which are commonly outsourced. Ensuring that adequate controls are in place is required regardless of whether that data is stored and processed in house or by an external party.

FYI

Although some service organizations may find an SOC engagement to be expensive and difficult, they might find they have little choice. This is because SOX Section 404 requires management to certify financial controls, even if they have been outsourced to a third party. Because an SOC 1 report can fulfill this obligation, organizations are demanding it from those to whom they outsource their operations.

SOC reports take the form of three different engagements, which product three different reports. The following are the three types of engagements and associated SOC reports:

- **SOC 1, Report on Controls at a Service Organization Relevant to User Entities' Internal Controls over Financial Reporting**—These reports are based on **Statement on Standards for Attestation Engagements No. 16 (SSAE 16)**. This has replaced what was commonly known as Statement on Auditing Standards (SAS) No. 70, or SAS 70. This report is intended to provide assurance to organizations (user entities) that rely on the service provider. Auditors of the user entities employ these reports in performing financial audits. There are two types of SOC 1 reports—Type 1 and Type 2. A Type 1 report includes the auditor's assessment whether the description of the service organization's system is fair as of a specific date. A Type 2 report is similar but also reports on the effectiveness of the controls through a specific period.

- **SOC 2, Report on Controls at Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy**—A SOC 2 report was specifically created to address the wide and growing use of technology and cloud-based providers. As the name of the report implies, the SOC 2 considers the security, availability, integrity, confidentiality, and integrity of the service organization's system and data. As with SOC 1, there are two types of SOC 2 reports: Type 1 and Type 2. A Type 1 report provides management's description of the organization's systems and the suitability of controls. A Type 2 report does the same, but also includes management's assessment of the controls' effectiveness.
- **SOC 3, Trust Services Report for Service Organizations**—SOC 3 is similar to SOC 2 but may be more appropriate for a service provider when the provider's customers don't have the need or knowledge to use the details provided by SOC 2. Unlike SOC 1 or SOC 2 reports, which are intended for specific audiences or restricted, SOC 3 reports can be freely distributed.

Table 4-1, adapted from the AICPA's "SOC Reports Information for CPAs," provides a comparison between the three different SOC types. Further, the AICPA Web site (<http://www.aicpa.org>) provides comprehensive information and valuable SOC guides and publications.

Although SOC 1 reports have effectively replaced SAS 70 reports since about 2010, they continued to be called SAS 70 reports even many years later. If that wasn't confusing enough, the SOC 1 report is also commonly referred to as SSAE 16, which again is the standard on which the SOC 1 brand is based. Finally, it's important to point out that an SOC 1 report, as was the original intent of the SAS 70, is strictly related to internal controls over financial reporting. Over the decades, however, SAS 70 has come to be a means for assuring the existence of adequate information security controls in general based on recommended practices. This need is largely AICPA's intent behind the SOC 2. In the absence of any true relationship of internal controls over financial reporting, an SOC 2 would be most appropriate for user entities that deal with many IT providers—and specifically the growing cloud service providers. Thus far, however, the trend has still been focused on SOC 1 compliance. While SOC 1 and its predecessor are well understood and accepted, the others have yet to fully mature.



WARNING

User organizations should not view an SOC report as a "rubber stamp" of approval for information security controls based on recommended practices. The audit is an assessment of financial controls related to the service organization's stated objectives. User organizations should examine each report carefully.

TABLE 4-1 Comparison of SOC reports.

	SOC 1® REPORT	SOC 2® REPORT	SOC 3® REPORT
Controls affected	Financial	Security, availability, processing integrity, confidentiality, or privacy	Security, availability, processing integrity, confidentiality, or privacy
Associated attestation standard	AT 801, Reporting on Controls at a Service Organization (Based on SSAE 16)	AT 101, Attestation Engagements	AT 101, Attestation Engagements
Guidance and aids	<i>AICPA Guide, "Service Organizations: Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting Guide"</i>	<i>AICPA Guide, "Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy"</i>	<i>AICPA Technical Practice Aid, "Trust Services Principles, Criteria, and Illustrations"</i>
Contents of report	Description of system and the auditor's opinion of the controls. A description of the auditor's test of the controls and results in a Type 2 report.	Description of system and the auditor's opinion of the controls. A description of the auditor's test of the controls and results in a Type 2 report.	Auditor's opinion of whether effective controls of the system have been maintained.

Source: American Institute of CPAs

► NOTE

The SOC 1 report (based on SSAE 16) replaced the SAS 70, yet many still refer to it by the old name even many years later or simply call it an SSAE 16 report.

ISO/IEC Standards

The **International Organization for Standardization (ISO)** is a nongovernment group that brings both the private and public sectors together and creates solutions for business and society. New standards are created by industries or ISO itself. When a particular industry identifies a specific need, it informs a technical committee within the ISO to get standards developed. If a committee does not exist, a new one may be set up. To be accepted, though, the members of the ISO technical committee must establish majority support and a global relevance must be set. The technical committees within ISO are composed of experts from specific industries such as technical and business. Additionally, other entities such as laboratories, government agencies, consumer organizations, and academia may join the committee experts.

ISO/IEC 27000 is a series of standards and related terms that provide guidance on matters of information security. This includes implementing, designing, and auditing an

information security management system (ISMS). An ISMS describes the policies, standards, and programs related to information security. These standards were established by the ISO and **International Electrotechnical Commission (IEC).** Other popular series include ISO 9000 and ISO 14000, which deal with quality management and environmental management, respectively. The technical committee directly responsible for the ISO 27000 series is ISO/IEC JTC1 (Joint Technical Committee 1) SC 27 (Subcommittee 27). This nomenclature is especially useful when browsing the standards catalog at the ISO Web site. The ISO/IEC JTC1 is the joint committee responsible for information technology. Within these are several subcommittees. Subcommittee 27 defines IT Security techniques. Other subcommittees include SC 37 for biometrics and SC 35 for user interfaces. Within just ISO/IEC JTC 1/SC 27 there are well over 100 published standards. The focus here is on the ISO 27000 series and specifically the first three standards.

Table 4-2 lists the published ISO/IEC standards in the ISMS family of standards. The next two sections provide details on ISO/IEC 27001 and 27002. Both of these standards focus on information security systems and processes, and are complementary to each other.

FYI

It is common in speech as well as in print to find these standards preceded only by "ISO" rather than "ISO/IEC," used throughout this chapter. The 27000 series is also called the ISMS family of standards and is often shortened to ISO27k.

TABLE 4-2 ISO/IEC 27000 ISMS family of standards.

TYPE OF STANDARD	PUBLISHED STANDARD	DESCRIPTION
Vocabulary	27000	Information security management systems—overview and vocabulary
Requirement	27001	Information security management systems—requirements
	27006	Requirements for bodies providing audit and certification of information security management systems
Guideline	27002	Code of practice for information security controls
	27003	Information security management system implementation guidance
	27004	Information security management—measurement
	27005	Information security risk management
	27007	Guidelines for information security management systems auditing
	27008	Guidelines for auditors on information security controls
	27013	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
	27014	Governance of information security
	27016	Information security management—organizational economics
Sector-specific guideline	27010	Information security management for inter-sector and inter-organizational communications
	27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
	27015	Information security management guidelines for financial services
	27018	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

	27019	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
	27779	Information security management in health using ISO/IEC 27002
Control-specific guideline	27031	Guidelines for information and communication technology readiness for business continuity
	27032	Guidelines for cybersecurity
	27033	Network security—multipart
	27034	Application security—multipart
	27035	Information security incident management
	27036	Information security for supplier relationships—multipart
	27037	Guidelines for identification, collection, acquisition, and preservation of digital evidence
	27038	Specification for digital redaction
	27039	Selection, deployment, and operations of intrusion detection systems (IDSe)
	27040	Storage security

ISO/IEC 27001 Standard

ISO/IEC 27001 is a worldwide standard formally known as “ISO/IEC 27001:2013—Information Technology—Security Techniques—Information Security Management Systems—Requirements.” It was originally established in October 2005 as ISO/IEC 27001:2005 and replaced British Standards Institute Security Management Standard BS7799-2.

NOTE

ISO/IEC 27001 is not a control standard. It focuses on management and processes, and relies upon other standards such as ISO/IEC 27002. ISO/IEC 27002 focuses on the specific controls to make ISO/IEC 27001 possible.

ISO/IEC 27001 is the best-known specification in the ISMS family of standards. It contains accepted good practices and provides an accepted baseline against which IT auditors can audit. It specifies the auditable requirements for establishing, applying, operating, maintaining, reviewing, monitoring, and improving a control framework based on an organization’s information security risk. Such risk applies to the information structure within the organization. This includes, for example, management responsibility and documentation. It also applies across all departments, such as human resources, facilities, and operations. It looks at the entire organization and its information assets and walks through a process to determine the associated risks. The process calculates the risk and impact to the organization. Then, it considers the steps needed to remove, reduce, or accept the risk.

The requirements established in ISO/IEC 27001 cover all styles of organizations, such as large enterprises to small- and medium-sized businesses. This also includes federal agencies and not-for-profit organizations. Although ISO does not perform certifications, it is common for organizations to assert that a product or system is certified to an ISO standard. This may be done by an accredited certification body. Many organizations choose to not become certified, yet still implement the standard. Becoming certified does often lend credibility, but it

is is certainly not required. Organizations will still benefit from the good practices either way. Further, certification makes it clear that the organization has done the following:

WARNING

Unlike many other standards and frameworks, the ISO standards are not free of charge. ISO charges fees for the standards, and ISO maintains a prohibitive copyright stance.

- Performed due diligence
- Ensured that information controls meet the organization's needs on an ongoing basis
- Considered risks associated with the organization

According to the ISO organization, ISO/IEC 27001:

specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

In other words, ISO/IEC 27001 provides the high-level framework upon which an organization can implement an ISMS. Optionally, the specification serves as the framework by which accredited auditing organizations may conduct a formal assessment for the purpose of certification.

The contents of ISO/IEC 27001 is made up of the following sections and annex:

- **Introduction**—This section briefly summarizes the intent of the standard, which is to establish a continuous process for an ISMS.
- **Scope**—This section specifies that ISMS is applicable to all organizations.
- **Normative references**—This section provides references to other documentation that plays a major role in implementing the standard.
- **Terms and definitions**—This section simply references ISO/IEC 27000, which defines the vocabulary.

PDCA

Plan-do-check-act (PDCA) is a significant ongoing approach for continuous improvement. While the latest version of ISO/IEC 27001 no longer directly incorporates the PDCA model, it was a well-known fixture in ISO/IEC 27001:2005. PDCA also is known by other names, including Shewhart cycle, Deming cycle, or Deming wheel. This approach is popular in varying situations focused on continuous improvement. It is also applied when defining a repetitive work process.

Although not invented by Dr. W. Edwards Deming, he certainly popularized its use. Deming, often called the father of quality management, is known for his work in quality improvement. He is credited with having been the driving force behind Japan's reputation for quality products. He later had a profound impact in the United States.

The four steps within PDCA are conceptually simple. Deming actually called this four-step process the ***Shewhart cycle*** after Walter A. Shewhart, an accomplished statistician. The key principle of the PDCA is

iteration. With each cycle completed, the knowledge about the underlying system being studied improves. Repeating the process brings perfection closer.

While the PDCA model has been removed from the latest version, the ideas still exist. In fact the sections for planning, support, operation, performance evaluation, and improvement within ISO/IEC 27001:2013 demonstrate that the PDCA model is still very much alive.

- **Context of the organization**—This section lists the internal and external factors that influence the goals of the ISMS.
- **Leadership**—This section emphasizes the need to establish and communicate management responsibility.
- **Planning**—This section explains the need to establish information security objectives, along with how those objectives will be achieved.
- **Support**—This section outlines the required support and documentation needed.
- **Operation**—This section details the requirements for assessing the efficiency and effectiveness of the ISMS.
- **Performance evaluation**—This section discusses the opportunity to make improvements through monitoring and measuring controls, processes, and management.
- **Improvement**—This section addresses the need for issues to be identified and quantified so corrective action can be applied.
- **Annex A**—This provides a listing of controls and control objectives, which are related to those found ISO/IEC 27002.

NOTE

ISO/IEC 27001 certification is not a one-time exercise. To maintain the certification, organizations must undergo ongoing review and monitoring of the ISMS.

FYI

ISO/IEC 27002 came from a UK government document originally published in 1995. The original document was republished as British Standard (BS) 7799. This was later republished by the ISO in 2000 as ISO 17799. This standard was updated in 2005 and finally renamed to bring it within the 27000 series of information security standards. The final document today is ISO/IEC 27002.

ISO/IEC 27002 Standard

ISO/IEC 27002 is formally known as “ISO/IEC 27002:2013 Information Technology—Security Techniques—Code of Practice for Information Security Management.” Whereas ISO 27001 formally defines mandatory requirements for an ISMS, ISO/IEC 27002 provides the suitable information security controls within the ISMS. ISO/IEC 27002 is merely a code of practice or guideline rather than a certification standard. Thus, organizations are free to select and put in place other controls as they see fit. While at the core, ISO/IEC 27001 provides the suitable controls for use within an ISMS, it is often used within a context outside of a formal ISMS. It also serves a couple other purposes. For example, organizations use ISO/IEC 27001 as a generic framework for commonly accepted controls or as a baseline for

developing controls.

Eighteen sections make up ISO/IEC 27002. The introduction and the first four sections provide introductory material, whereas the rest of the sections provide the core recommendations and controls. Sections 5 through 18 provide the following framework:

- Overview of organizational goals being addressed
- List of practical controls
- Guidance for how to put in place each of the controls
- Additional information, including cross-references within the standards and other standards

The preceding framework applies to the key sections within the documents, which are summarized in the following list:

- **Information Security Policies**—Covers management guidance and the need to have a documented information security policy and review process
- **Organization of Information Security**—Covers the organization of information security as related to the internal organization parties and mobile devices and teleworking
- **Human Resource Security**—Covers employment of employees and those associated with an organization regarding preemployment checks, termination, and change of employment
- **Asset Management**—Covers the discovery and classification of assets and information, including how to handle media
- **Access Control**—Covers business requirements, user controls and responsibilities, application-level controls, and access controls for networks and operating systems
- **Cryptography**—Covers cryptographic controls, including both the policy on the use of cryptography and key management
- **Physical and Environmental Security**—Covers secure facilities and equipment security
- **Operations Security**—Covers the largest range of areas, including operational procedures such as change and capacity management; malware, backup, operational software controls, and vulnerability management; and audit, logging, and monitoring
- **Communications Security**—Covers network security management and information transfer
- **Systems Acquisition, Development, and Maintenance**—Covers systems development and acquisition, including security requirements of systems, correct processing applications, and test data
- **Supplier Relationships**—Covers information security and managing aspects related to third parties or suppliers
- **Information Security Incident Management**—Covers information security incident management, including reporting of events and security weaknesses and improvements
- **Information Security Aspects of Business Continuity Management—Covers protecting critical processes from disruption**
- **Compliance**—Covers complying with legal requirements, security policies, standards and technical compliance, and considerations for information systems audits or reviews

Each of the preceding key topics ISO 27002 is composed of many individual controls detailed in the standard. This standard provides wide coverage across the information security domain, and is quite specific in the prescription of controls. As a result, the security community has embraced it widely.

NIST 800-53

The Federal Information Security Management Act of 2002 (FISMA) tasked the National Institute of Standards and Technology (NIST) with developing security standards and guidelines for the federal government. Two documents that are addressed here include the following:

- NIST 800-53, Recommended Security Controls for Federal Information Systems
- NIST 800-53A, Guide for Assessing the Security Controls in Federal Information Systems

NIST 800-53 provides a comprehensive catalog of security controls. **NIST 800-53A** provides a framework for assessing the adequacy of in-place controls. Although both are targeted to the federal government, many organizations appreciate the depth and prescriptive nature of the NIST standards. As a result, they are widely used outside of government, even if used as a complement to other standards such as ISO/IEC 27002. NIST 800-53 addresses a wide range of controls. The controls consider multiple aspects, including management, technical, and operational. The catalog of controls is grouped into 17 families of controls, which include the following:

NOTE

NIST works with the public and private sectors to establish relationships between NIST's security controls and those provided by ISO 27002, for example.

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- Security Assessment and Authorization
- System and Services Acquisition
- System and Communication Protection

- System and Information Integrity

The framework for each of the preceding families of controls is composed of the following elements:

- **Control**—A descriptive statement of the security measure to be put in place
- **Supplemental guidance**—Additional guidance for consideration
- **Control enhancements**—Information on augmenting the control with additional functionality or increased security
- **References**—A listing of related federal laws, executive orders, directives, policies, standards, and guidelines related to the control
- **Priority and baseline allocation**—A listing of codes used for prioritizing decisions during security control implementation and control enhancements for systems of varying degrees of impact

NIST 800-53A provides guidance for building effective security assessment plans. This standard is an excellent complement to NIST 800-53. NIST 800-53A is designed to conduct assessments within a risk-management framework and provides the following:

- Information about the effectiveness of security controls applied
- Proof of the quality of the risk-management process in use
- Information about the strengths and weaknesses of the information systems

This standard discusses in detail the process for conducting assessments. This includes topics on preparing for the assessment, developing the plans, conducting the assessment, and follow-on reporting, analysis, and other activities.

Cybersecurity Framework

In 2014, NIST released the first version of what is known as the **Cybersecurity Framework**. This framework is a result of President Barak Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," issued in 2013. The development of the framework is a result of collaboration between both government and private-sector participants, given the vested interests and associated stakeholders.

The purpose of the Cybersecurity Framework is to provide a voluntary structure for reducing the risks to critical infrastructure. The first version considers various other standards and best practices, and "provides a common language and mechanism for organizations" to do the following five key items:

- Describe their existing cybersecurity stance.
- Describe their ideal end state for cybersecurity.
- Prioritize areas for improvement as related to managing risk.
- Measure progress toward the ideal end state.
- Encourage communication among the various stakeholders.

The Cybersecurity Framework is made up of three components:

- The Framework Core

- The Framework Profile
- The Framework Implementation Tiers

The Framework Core is a matrix of activities and associated references. The framework includes various categories across five different functions. These functions are as follows:

- Identify
- Protect
- Detect
- Respond
- Recover

For each of the categories or subcategories across one of the aforementioned functions, references are included. References draw on existing standards, guidelines, and best practices. The framework includes an example for the Protect function. Within the Protect function are various categories, such as Data Security and Access Control. For example, ISO/IEC 27001 provides control A.8.8.3 for physical media transfer. This control serves as an informative reference to the Data Security subcategory and specifically addresses the subcategory “Data during transportation/transmission is protected to achieve confidentiality, integrity, and availability goals.”

The Framework Profile provides the primary mechanism to improve the security posture by comparing the existing state or profile with the ideal end state or target profile. Finally, the Framework Implementation Tiers define four levels, which describe how an organization manages risk. The following are the tiers in order from least mature to most:

- **Tier 1**—Partial
- **Tier 2**—Risk informed
- **Tier 3**—Risk informed and repeatable
- **Tier 4**—Adaptive

Various frameworks, and especially the Cybersecurity Framework, consider that organizations may use or reference multiple frameworks and standards. The Cybersecurity Framework is purposely designed to supplement these other programs. Further, it can be used by organizations just starting out or to improve existing programs.

Developing a Hybrid Auditing Framework or Approach

Frameworks such as COSO and COBIT allow audited organizations to use the same approach for internal audits as they do for external audits. In addition, these frameworks allow traditionally operations-focused audits to combine with traditionally IT-focused audits. This provides the basis for a hybrid or **integrated audit**.

The need for integrated audits is largely driven by Sarbanes-Oxley, which established the Public Company Accounting Oversight Board (PCAOB). The PCAOB oversees the rules that apply to publicly traded companies. Traditionally, auditors examined and expressed their opinions on a company’s financial statements. However, the rules now require auditors to express an opinion regarding the organization’s controls over financial reporting. For example, **Auditing Standard No. 5** states that as part of evaluating financial reports, the auditor should assess the following:

- The inputs, procedures, and outputs of the processes used to produce financial statements
- The amount of IT involvement in the financial reporting process



WARNING

Although an integrated approach allows auditors to use the work of others, caution is advised. The previous work of those with a low degree of objectivity or a low degree of competence should not be used. Individuals or groups with compliance or testing responsibilities will be more useful for external auditors. Regardless, the degree of risk associated with a particular control should always be considered. The higher the risk, the more likely it is that the auditors should verify the control's effectiveness themselves.

The standard also explicitly states that the “audit of internal controls over financial reporting should be integrated with the audit of the financial statements.” The standard continues, “The auditor should design his or her testing of controls to accomplish the goals of both audits simultaneously.”

Auditing Standard No. 5 allows the use of the work of others. This can save both time and resources. For the purpose of the audit of internal controls, external auditors may use the work of others. They may also receive direct assistance. This includes internal auditors, company personnel, or third-party organizations working under the direction of management or the audit committee.

Some of the key requirements to developing such an approach require organizations to do the following:

- Select appropriate frameworks.
- Adopt risk-based approaches.
- Map business processes to IT processes.
- Have internal audits use the same approach as external audits.

COSO provides an excellent starting point. COSO provides a framework based on risk and is an “integrated framework.” COBIT is, then, a logical next step. COBIT takes the COSO objectives and turns them into a framework applicable to IT.



CHAPTER SUMMARY

As you have seen, there are various standards and frameworks. Each has a common goal of establishing sensible practices within the organizations that use them. Standards and frameworks have different advantages and disadvantages. Some, such as COSO, appeal to senior-level positions. Others, such as ISO/IEC 27002, provide controls that are more prescriptive and will appeal to those managing and implementing systems security. Because of the differences, organizations and auditors will find that a combination of standards and frameworks will be most appropriate. Both auditors and organizations benefit greatly from using well-known standards and frameworks. This includes reduced costs, and allows the auditor and the organization being audited to better understand one another. Finally, it provides the basis for integrated auditing.



KEY CONCEPTS AND TERMS

Auditing Standard No. 5

Committee of Sponsoring Organizations (COSO) of the Treadway Commission

Control activities

Control objectives

Cybersecurity Framework

Descriptive control

Enterprise risk management (ERM) framework

Framework

Information security management system (ISMS)

Information Technology Assurance Framework (ITAF)

Information Technology Governance Institute (ITGI)

Integrated audit

International Electrotechnical Commission (IEC)

International Organization for Standardization (ISO)

ISACA

ISO/IEC 27001

ISO/IEC 27002

NIST 800-53

NIST 800-53A

Plan-do-check-act (PDCA)

Prescriptive control

Risk IT Framework

Service Organization Control (SOC) reports

Statement on Standards for Attestation Engagements No. 16 (SSAE 16)

Val IT Framework



CHAPTER 4 ASSESSMENT

1. A _____ is a conceptual set of rules and ideas that provide structure to a complex and challenging situation.
2. Frameworks differ from each other in that they might offer varying levels of depth and breadth.
 - A. True
 - B. False
3. Avoiding the need for audits is one reason organizations develop clearly documented policies, standards, and procedures.
 - A. True
 - B. False
4. Which of the following should organizations do when selecting a standard? (Select three.)
 - A. Select a standard that can be followed.
 - B. Employ the selected standard.
 - C. Select a flexible standard.
 - D. Select a standard that other organizations in the same geographic location are using.

- 5.** The COSO framework is targeted to which of the following groups within a company?
- A. Executive management
 - B. First-line management
 - C. Security analysts
 - D. Application developers
- 6.** COSO is the acronym for which of the following?
- A. Compliance Objectives Standards Organization
 - B. Committee of Sponsoring Organizations
 - C. Compliance Organization Standard Operation
 - D. Committee on Standard Objectives
- 7.** Responding to business requirements in alignment with the business strategy is an example of an IT _____.
- 8.** Which one of the following is *not* true of COBIT?
- A. It is business-focused.
 - B. It is security-centered.
 - C. It is process-oriented.
 - D. It is controls-based.
 - E. It is measurement-driven.
- 9.** Which one of the following is *not* one of the four domains of COBIT?
- A. Plan and Organize
 - B. Implement and Support
 - C. Acquire and Implement
 - D. Deliver and Support
 - E. Monitor and Evaluate
- 10.** SSAE 16 Type 1 includes everything in a SSAE 16 Type 2 report, but it adds a detailed testing of the controls over a specific time frame.
- A. True
 - B. False
- 11.** Organizations may be audited for both ISO/IEC 27001 and ISO/IEC 27002 and receive a formal certification for each.
- A. True
 - B. False
- 12.** ISO/IEC 27002 is a code of _____ for information security management.
- 13.** What PCAOB standard states that the auditor should assess the amount of IT involvement in the financial reporting process?
- A. Auditing Standard No. 1
 - B. Auditing Standard No. 11
 - C. Auditing Standard No. 55
 - D. Auditing Standard No. 5
- 14.** Which of the following provides a framework for assessing the adequacy of implemented controls?
- A. NIST 800-53
 - B. NIST 800
 - C. NIST 800-53A
 - D. NIST 800A

CHAPTER 5

Planning an IT Infrastructure Audit for Compliance

A

UDIT PLANNING SHOULD NOT BE OVERLOOKED. What goes into the planning process

directly affects the quality of the outcome. The planning stage is the first step and takes place before any of the detailed audit work begins. A proper plan ensures that resources are focused on the right areas and that potential problems are identified early. A successful audit first outlines what's supposed to be achieved as well as what procedures will be followed and the required resources to carry out the procedures.

Although each audit will vary, the plan and approach to each audit follow similar characteristics. Despite the best plans, however, circumstances do change, and plans need to be adjusted. As a result, flexibility must be considered. Significant errors, suspected fraud, and misrepresentation can all have a considerable effect upon the initial plan. Regardless, proper planning helps ensure an effective and timely audit.

Chapter 5 Topics

This chapter covers the following topics and concepts:

- How to define the scope, objectives, goals, and frequency of an audit
- What the critical requirements for an audit are
- How to assess IT security
- How to obtain information, documentation, and resources
- How to map the security policy framework definitions to the seven domains of IT infrastructure
- How to identify and test monitoring requirements
- How to identify critical security control points that must be verified throughout the IT infrastructure
- How to build a project plan

Chapter 5 Goals

When you complete this chapter, you will be able to:

- Define the scope and frequency of an audit
- Identify the key requirements for an audit
- Understand the importance of risk management in assessing security controls
- Identify the information and resources needed for an IT audit
- Relate the IT security policy framework to the seven domains of IT infrastructure
- Understand why monitoring requirements help with an IT audit
- Identify security control points

- Differentiate between the project management tasks of an IT audit

Defining the Scope, Objectives, Goals, and Frequency of an Audit

The scope, objectives, goals, and frequency of audits are based on a risk assessment. Depending on the risk, the frequency of audits varies. Critical systems controls might need to be monitored more often than noncritical controls. In more high-risk situations, automated or continual audit tests might be considered.

Prior to performing an audit, the auditor should first define the **audit scope**. The scope includes the area or areas to be reviewed as well as the time period. Experienced auditors know it's just as important to define what will be audited as it is to define what will not be audited. If scope is not clearly defined, **scope creep** occurs, likely increasing the auditor's workload. Scope creep is a term common to projects where the plans or goals expand beyond what was originally intended.

The **audit objective** is the goal of the audit. Both scope and objective are closely related. For the audit to be effective, the scope must consider the objectives of the audit. Defining scope requires consideration of the personnel, systems, and records relevant to the objective. Time is another consideration dependent upon the objective. The depth and breadth of an audit usually determines the time frame required to meet the objectives.

An external audit of financial controls, for example, will likely have a more narrow scope than an internal audit of information technology (IT) controls. When defining the scope, the auditor should consider the controls and processes across the seven domains of IT infrastructure. This includes relevant resources such as the following:

- Data
- Applications
- Technology
- Facilities
- Personnel

It is important for auditors to ensure the scope is sufficient to achieve the stated objectives. Restrictions placed on the scope could seriously affect the ability to achieve the stated objective. Examples of restrictions that an organization may place on an auditor that could have such a negative impact include the following:

- Not providing enough resources
- Limiting the time frame
- Preventing the discovery of audit evidence
- Restricting audit procedures
- Withholding relevant historical records or information about past incidents

Project Management

An audit is a project. As with any project, proper planning is necessary. Auditors should be familiar with the Project Management Institute (PMI), which has created a standard named *A Guide to the Project Management Body of Knowledge (PMBOK)*. This guide provides a well-known and applied framework for managing successful projects.

A project, such as an audit, has three important characteristics. First, a project is temporary. This means it has an identified start and end date. Unlike operations or a program, a project lasts for a finite time period. Second, a project is unique and produces unique results. At the end of the project, a deliverable is produced. Although projects might be similar, the process, resources, constraints, and risks, for example, will differ. Finally, a project is progressively elaborated. Because each project is unique, the process is more dynamic. Projects will occur in separate steps. As the process continues, the next phase becomes clearer.

Projects require someone to manage them. This position is often given the title of project manager. Large projects and even audits might have a dedicated project manager. Other times, the person managing the project might be the project expert. Project management requires the management of three competing needs to achieve the project objectives. Known as the *triple constraint*, these include scope, cost, and time. Consider, for example, a project with a large scope, but with little time and cost. More than likely, quality will be compromised. A project manager must be aware of all three constraints at the start of and throughout the project.

Planned audit activities also have a defined rate of occurrence, known as the **audit frequency**. There are two approaches to determine audit frequency. Audits can occur on an annual basis or every two or three years, depending on regulatory requirements and the determined risk. IT audits also are known for not following a predefined frequency, but instead using a continuous risk-assessment process. This is more appropriate given the fast-paced change in technology as well as the threats and vulnerabilities related to IT.

Identifying Critical Requirements for the Audit

The risk assessment will influence the critical requirements for an IT audit. Overall, there are various types of IT audits. In addition to infrastructure audits for compliance, other examples include audits specific to IT processes, such as governance and software development. Another example includes integrated audits, where financial controls are the focus.

Auditing IT infrastructure for compliance incorporates the evaluation of various types of controls. IT organizations today are concerned with controls relating to both security and privacy. Traditionally, privacy and information security activities are separate activities. The two, however, have become more interrelated, and coordination between the two has become a priority for many organizations. Two major factors contributing to this are regulatory issues and the rapid growth and widespread use of the Web. As a result, both privacy and information security are converging, specifically around compliance issues.

Implementing Security Controls

Before an evaluation of controls can begin, the auditor must first identify the critical controls. To do so, the auditor must consider the audit scope and objective along with the risk assessment. Documentation and any preliminary interviews also help to identify the requirements.

Controls can be classified into different groups to aid in understanding how they fit into the overall security of a system. [Figure 5-1](#) illustrates the different dimensions of control classifications. Understanding the classifications provides auditors with a foundation to identify and assess critical controls.

A high-level classification of controls for IT systems includes general and application controls. General controls are also known as infrastructure controls. These types of controls apply broadly to all system components across an organization. Application controls apply to individual application systems. Types of application controls include various transaction

controls, such as input, processing, and output controls.

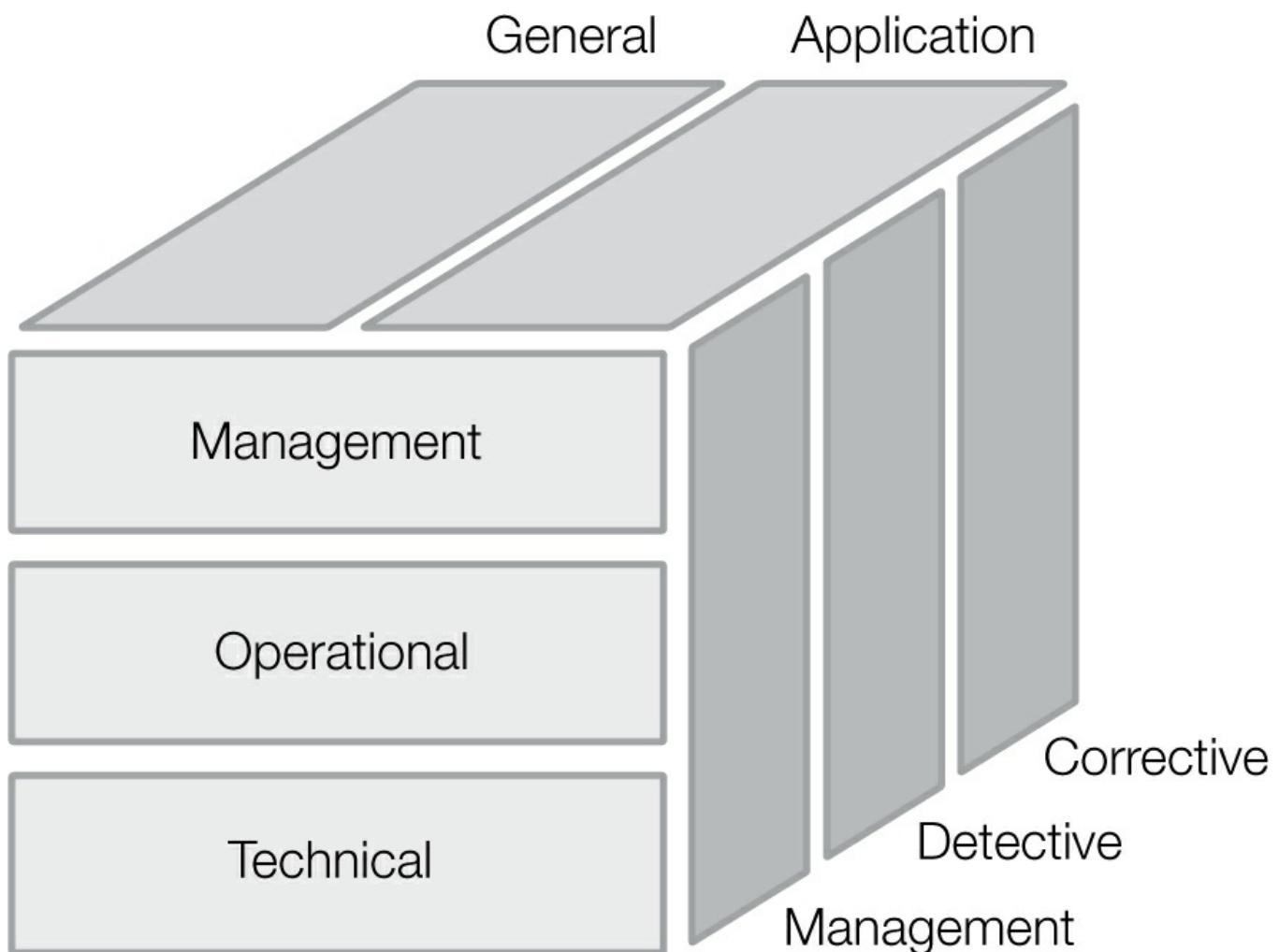


FIGURE 5-1 Control classifications.

Three IT security controls covered by the National Institute of Standards and Technology (NIST) include management, operational, and technical controls. The following list provides a description and examples of each of these:

- **Management controls**—These include controls typically governed by management as part of the overall security program. Examples include the following:
 - Security policy
 - Security program management
 - Risk management
 - Security and planning in the system development life cycle
 - Assurance
- **Operational controls**—These include controls that are implemented by people rather than systems. These controls are often interrelated with both management and technical controls. Examples include the following:
 - Personnel and user issues
 - Contingency and disaster planning
 - Incident response and handling
 - Awareness, training, and education

- Computer support and operations
- Physical and environmental security
- **Technical controls**—These include controls that are performed by the IT systems. Examples include the following:
 - Identification and authorization
 - Logical access control
 - Audit trails
 - Cryptography

Controls are further classified as being preventive, detective, or corrective. Preventive controls stop a particular threat in the first place. A door lock on a home is a simple example of a preventive control. A detective control identifies that a threat is present. A home alarm system, for example, is a common detective control. (Some people even advertise they have an alarm system by putting a notice on the door or a sign in the yard. In this case, this also serves as a preventive control.) Finally, a reactive or corrective control can lessen the effects of a threat. A home alarm system that also notifies the police department is an example of a reactive control.

NOTE

Antivirus software is a common control that spans all three controls. It can prevent a system from getting a virus in the first place. It can detect if a virus is on the system. Finally, it can react and correct the situation by removing or quarantining the virus.

Protecting Privacy Data

Audits of IT infrastructure relating to security are common. However, due to recent legislation regarding the need to protect personally identifiable information, audits specific to privacy are more commonplace than before. ISACA defines privacy within the context of information systems as “adherence to trust and obligation in relation to any information relating to an identified or identifiable individual (data subject). Management is responsible to comply with privacy in accordance with its privacy policy or applicable privacy laws and regulations.”

Privacy audits go beyond traditional IT audits in that the entire information lifecycle process needs to be considered. This includes not just the controls relating to how it was gathered and secured, but also how it is collected, used, and retained. Specifically, privacy audits address the following three concerns:

- What type of personal information is processed and stored?
- Where is it stored?
- How is it managed?

[Table 5-1](#) outlines guidance for privacy audits established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). This guidance is named **Generally Accepted Privacy Principles (GAPP)**.

A privacy audit should consider what privacy laws apply to the organization. Auditors should consider who has responsibility for privacy within the organization. This includes the roles of legal counsel and whether a **chief privacy officer (CPO)** role is established. (The CPO is

a senior-level position responsible for the overall management of an organization's privacy program.) Finally, the policies and procedures specific to privacy should be examined.

TABLE 5-1 The Generally Accepted Privacy Principles.

PRINCIPLE	DESCRIPTION
Management	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
Notice	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
Choice of consent	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
Collection	The entity collects personal information only for the purposes identified in the notice.
Use and retention	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as is necessary to fulfill the stated purposes.
Access	The entity provides individuals with access to their personal information for review and update.
Disclosure to third parties	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
Security for privacy	The entity protects personal information against unauthorized access.
Quality	The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
Monitoring and enforcement	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Assessing IT Security

Examining IT security is a key component of auditing IT infrastructure for compliance. An audit can help identify fraud, ineffective IT practices, improper use of resources, and inadequate security. Assessing IT security is largely about ensuring that adequate controls are in place. Controls cost money, however. The selection and implementation of controls must be a result of a consideration of risk.

Suppose you want to build a fence to protect a cow. Building the fence will cost money. Exactly how much money it will cost might depend upon the quality and size of the fence. How much might you be willing to spend? Of course, you should first understand why you want to protect the cow. How valuable is this cow to you? What are you protecting the cow from? Let's assume the cow has some type of value to you—otherwise, there would be little reason to spend money on protecting the cow. Is a fence the only solution? Could you tie the cow to a tree instead? If you decide to build the fence, is it strong enough? Is it high enough? Now suppose you decide to have the security of your fence assessed. What you *don't* need is for the auditor to come by and tell you what you already know—that you have a fence in place. Rather, what would be useful is a determination of the lack of controls, the ineffectiveness of controls, or even the use of unnecessary controls. If your cow turns out to be a bull, for example, perhaps that fence won't be so effective. Is the fence effective against someone determined to steal the cow? To understand these issues, consider the following:

- Is a control even required?
- How much effort or money should be spent on a control?
- Is the control effective?

Understanding the answers to these questions requires thought about risk. This is why risk management needs to be a key part of organizations and any audit.

Risk Management

Managing and understanding risk is a key operating component of any organization. Risk is about uncertainty. Yet, there will always be uncertainties across organizations. Uncertainty presents both challenges and opportunities for companies. Risk management provides a method for dealing with the uncertainty. This includes identifying which ones to accept and which ones to control. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission, which provides a framework for **enterprise risk management (ERM)**, identifies the following key components of ERM:

- **Aligning risk appetite and strategy**—This helps the organization to manage the uncertainty with consideration of the goals of the organization.
- **Enhancing risk response decisions**—This improves the organization's ability to make decisions about how to better manage risk.
- **Reducing operational surprises and losses**—This enhances the organization's ability to identify potential events or threats and react appropriately.
- **Identifying and managing multiple and cross-enterprise risks**—This helps the organization to consider related risks from across the organization and provides a unified response across the varying risks.
- **Seizing opportunities**—This helps the organization to recognize events from which new opportunities can be pursued.
- **Improving deployment of capital**—This improves how organizations divide their financial resources to enhance performance and profitability.

An example of an IT risk framework compatible with ERM is ISACA's Risk IT. The Risk IT framework is completely covered with the Control Objectives for Information and Related Technology (COBIT) framework. Risk IT provides a comprehensive framework not just for assessing risk, but also for governance and response. Combined with Risk IT and another framework, Val IT, COBIT 5 provides a framework of controls to minimize as well as manage risk. Another example of an information security risk management framework is ISO standard **ISO/IEC 27005**. In addition to providing guidelines for information security risk management, this ISO standard also supports the concepts within ISO/IEC 27001.

The key component of risk management includes a risk assessment. Planning an audit of IT infrastructure depends on this assessment. The audit plan should be prepared only after a risk assessment is complete. The key reason for this is that the audit will focus on those areas with the highest risk.

There are several methodologies for assessing risk specific to IT environments. **NIST 800-30**, “Risk Management Guide for Information Technology Systems,” is one such example. This guide provides a practical nine-step process, as follows:

- **System characterization**—Identify and understand the systems and their operating environment.

- **Threat identification**—Identify potential methods or situations that could exploit a weakness.
- **Vulnerability identification**—Identify flaws or weaknesses that can be triggered or exploited, which might result in a breach.
- **Control analysis**—Analyze controls to reduce the likelihood of a threat successfully exploiting a vulnerability.
- **Likelihood determination**—Determine the likelihood of an attack by considering the motivation and capability of the threat source along with the nature of the vulnerability in relation to the current controls.
- **Impact analysis**—Determine the impact of a successful attack on a vulnerability by a threat. Consider the mission of a system, data criticality, and data sensitivity.
- **Risk determination**—Consider the likelihood, magnitude of impact, and adequacy of controls as an equation of risk.
- **Control recommendations**—Consider controls to reduce the level of risk to an acceptable level.
- **Results documentation**—Document for management the observations on threats and vulnerabilities as well as risks overall and recommended controls.

Evaluating risk requires looking at the different parts of the risk equation. Effective risk management starts with identifying the IT assets and their value. Next, organizations need to identify the threats and vulnerabilities to these assets. A **threat** is any activity that represents a possible danger. A **vulnerability** is a weakness. An analysis or assessment of both threats and vulnerabilities is a key part of the risk-management process. Next, organizations need to identify the likelihood each threat will exploit a vulnerability. Finally, organizations need to consider the impact of the risk. Risks should then be prioritized. This enables organizations to give attention to the most severe. Different methodologies are available, which provide clear frameworks for evaluating risk.

NOTE

Threats don't pertain to all organizations equally. This is part of what makes threat identification a difficult task. A simple example is the threat of a hurricane. Although a hurricane is a threat that can cause a loss, you wouldn't consider a hurricane a threat to a data center based in Iowa, for example.

Threat Analysis

Part of the risk-assessment process requires an examination of those activities that represent danger. Threats to IT are numerous and can affect the loss of confidentiality, integrity, and availability in a number of ways. Analyzing the potential threats requires the identification of all possible threats first. This is called **threat identification**.

Threats can be grouped as a combination of the following:

- Adversarial
- Accidental
- Structural
- Environmental

Information about threats such as natural disasters is readily available and easily obtained through private and governmental resources. The threats that are more difficult to identify are those that pertain specifically to the organization. Table 5-2 provides examples of various adversarial threat sources. The table includes a list of threats, motivations, and methods that might be used to carry out an attack. The methods are also known as **threat actions**.

All the threats in Table 5-2 represent varying degrees of potential risks if they are accompanied by vulnerabilities. Each organization will identify its unique threats. Even businesses with multiple locations will have threats specific to that location. To really understand threats, think about your own personal situation. What threats are common to you and where you live? Do these threats change as you travel? What threats exist based on your lifestyle and goals?

You need to consider likelihood when examining threats. Using the example of a hurricane earlier in this section, it is safe to say that the threat of a hurricane affecting the state of Iowa does not exist. The threat of a tornado, however, does exist. As a result, organizations should develop a threat classification mechanism. A simple example may include a classification of low, medium, and high:

- **Low**—No previous history of the threat, and the threat is not likely to occur
- **Medium**—Some history of the threat, and the threat might occur
- **High**—Substantial history of the threat, and the threat is likely to occur

TABLE 5-2 Examples of threats, motivations, and threat actions.

THREAT	MOTIVATION	THREAT ACTION
Cracker Criminal	Challenge Ego	Social engineering System intrusion
	Monetary gain Destruction of information	Computer crime Fraudulent act Information bribery
Terrorist	Destruction Exploitation Revenge	Bomb System penetration System tampering
Espionage	Competitive advantage Economic espionage	Economic exploitation Information theft Social engineering
Insiders	Curiosity Ego Revenge Unintentional errors	System bugs System sabotage Unauthorized access Computer abuse

Vulnerability Analysis

After performing a threat analysis, you need to identify weaknesses or flaws. Specifically, you need to identify vulnerabilities that can be exploited by the previously identified threats. This is known as **vulnerability analysis**. There are many ways to identify vulnerabilities. Examples include the following:

- Vulnerability lists and databases published by industry organizations
- Security advisories
- Software and security analysis using automated tools



TIP
The MITRE Corporation catalogs vulnerabilities in the Common Vulnerabilities and Exposures (CVE), which includes tens of thousands of items.

It is important to consider threats relative to vulnerabilities. Think about operating system patches issued by Microsoft or Apple. Typically, these fix potential vulnerabilities, which were previously unknown and have since been discovered. In most cases, these vulnerabilities affect a particular piece of the system. Say, for example, Microsoft issues a patch to fix a vulnerability for a particular service of the operating system. However, what if you don't use this service or the service is turned off? In this case, the vulnerability is not really vulnerable. What if the particular system you use does not and will never be connected to the Internet? In this case, the threat in question does not exist. This is why it is important to pair threats with vulnerabilities. Threats are matched with existing vulnerabilities to further understand the risk. Finally, likelihood and impact must be considered. What is the likelihood that a particular threat can exploit a specific vulnerability? If that occurs, what would be the impact?

Consideration of all these elements involves tradeoffs. For example, you can do many things to remove or reduce specific threats and vulnerabilities in your personal life, but you might choose not to. You might even choose not to apply specific controls that can reduce the risks. Many of these decisions are based on your goals and personal tradeoffs. As you consider these concepts, think about the following:

- Why do some people live in areas with higher crime rates?
- Why doesn't everyone wear a bulletproof vest?
- Why do you ride in or drive vehicles when there are approximately 40,000 vehicle deaths per year in the United States?
- Why do some people spend more money on home security systems than others?

Risk Assessment Analysis: Defining an Acceptable Security Baseline Definition

Given the previous inputs, the final step is to determine the level of risk. When pairing threats and vulnerabilities, risk is determined primarily by three functions:

- The likelihood of a threat to exploit a given vulnerability
- The impact on the organization if that threat against the vulnerability is achieved
- The sufficiency of controls to either eliminate or reduce the risk

At this point, matrixes and other mechanisms are useful for qualitatively understanding risk. Such matrixes typically categorize the impact and likelihood of threats as low, medium, or high. The product of this results in a risk being low, medium, or high.

An alternative approach is to analyze impact and likelihood *quantitatively*. Such matrixes might use percentage values or a numerical count instead of defining what is high versus medium. Quantitative risk analysis, while more accurate and objective, can also be more time-consuming and expensive.

Applying controls to a system helps eliminate or reduce the risks. In many cases, the goal is not to eliminate the risk. Rather, what's important is to reduce the risk to an acceptable level. Applying controls is a direct result of the risk-assessment process combined with an analysis of the tradeoffs. Several examples of the tradeoffs include the following:

- **Cost**—Are the costs of a control justified by the reduction of risk?
- **Operational impact**—Does the control have an adverse effect on system performance?
- **Feasibility**—Is the control technically feasible? Will the control be feasible for end users?

An effective risk-assessment process helps establish known good baselines for IT systems. A **baseline** is the system in a known good state, with the applied minimum controls relative to the accepted risk. Baselines provide a solid and simple method from which to audit a system. Comparing a system against a baseline can help identify nonexistent controls that should be applied as well as controls that have been removed or disabled. Additionally, a baseline audit can help identify a system that has been compromised or otherwise altered.

NOTE

The best security is layered. This means the information system is composed of multiple controls operating at different layers. This is similar to a castle and its location high on a hill surrounded by a moat, a series of walls, and then locks and guards.

An information system may have security controls at different layers in the system. For example, an operating system or network component typically provides an identification and authentication capability. An application may also provide its own identification and authentication capability, rendering an additional level of protection for the overall information system. As organizations select and specify security controls, they should consider components at all layers in the information system to provide effective security architecture and privacy.

In addition to the results of the risk assessment, numerous best-practice baselines exist to help organizations select appropriate security controls. These include the many documented standards from NIST. Several of these are introduced later in this chapter.

Obtaining Information, Documentation, and Resources

The COBIT framework provides a good starting point for auditors to assess IT controls. Before beginning an audit, however, the auditor needs to first gather information from people and relevant documentation as well as identify required resources. The information the auditor needs before performing an audit includes the following:

- An understanding of the organization and what its business requirements and goals are
- Knowledge of how the security program is currently in place
- Industry best practices for the type of organization and systems

Documentation related to business structure, configuration, and even previous audits should be gathered and reviewed. In many cases, auditors will need to request further documentation during the course of the audit. At any point, if the auditor is not given adequate documentation, the auditor should notify the responsible personnel.

In addition to understanding the regulatory and industry requirements to which the organization must adhere, auditors should have a much larger understanding of the business. General knowledge about the business can be gained by gathering information on business and reporting cycles, key business processes, and key personnel to interview.

Strategic objectives of an organization reveal details about the organization in the future and how this will affect its information systems. In addition, information about the operational objectives for internal control provides relevant information with regard to the current state of the organization.

An organization's written policies are among the most important documents for an auditor. They provide a guideline from which to check the environment for gaps. More specifically, the auditor can determine whether the organization is stating it is doing something that it is not.

There are many other types of documentation that should be gathered depending upon the scope of the audit across the seven domains of IT infrastructure. Examples include the following:

 **NOTE**

Documentation is a good sign that an organization has a sound security program in place. Other documents should include standards, procedures, previous audit reports, risk assessments, and network diagrams.

- Administrative documentation
- System documentation
- Procedural documentation
- Network architecture diagrams
- Vendor support access documents and agreements

Existing IT Security Policy Framework Definition

The results of an audit will reflect how well an organization is adhering to its security policy. However, risk management must be considered. How well an organization adheres to its own policy when combined with an assessment risk helps to identify any gaps. For example, are there control objectives not defined in the policy that should be?

Frameworks exist to help with risk-management programs, security programs, and policy creation. ISO/IEC 27002, for example, provides a structured way for organizations to determine their IT security policy. Accounting and audit firms traditionally had their own interpretations of security standards. They, however, have been increasing the use of existing frameworks for benchmarks. It is important for the auditor to know upon what framework an organization has based its policy. This allows better alignment between the organization's policy and the audit. Most internal audits, to ensure compliance across the IT infrastructure, will align with the comparable framework.

Many organizations now have taken steps to implement a security policy framework. However, there are still many instances in which the policy is not actually being enforced. Additionally, information security policies are living documents. Business environments change. Technologies change. Risks change. As a result, companies with existing policy frameworks might discover that their policies are outdated. The IT security policy must be managed as an ongoing program to evolve with changing requirements and ensure adherence.

 **NOTE**

An IT audit doesn't just assess adherence to the security policy; it also uncovers situations in which the policy needs to be refined.

TIP

It is a good practice to have executive management approve and sign each high-level policy and provide a statement about the importance of the policy and how it helps support the objectives and goals of the organization.

Finally, policies are fundamental to the organization's actions. The policies drive the behavior of the people within an organization and even the technologies acquired. One of executive management's responsibilities is to set goals. Management further supports these goals with a set of objectives. These objectives are communicated throughout the organization by policies. This applies not just to IT security policies but also to policies across the organization. The policies set the standards, which help drive the business to achieve its goals. An organization's policies are quite important if they are expected to drive actions and behaviors from the top down. Therefore, high-level policies should be approved and signed by executive management.

Configuration Documentation for IT Infrastructure

The auditor will gather documents related to the configuration of the systems being audited. Although a single system component is possibly made up of thousands of configuration elements, the following are examples of items the auditor should gather from documentation:

- Host name
- Internet Protocol (IP) addresses
- Operating system
- Patch level
- Hardware specifications
- Installed software
- Protocols
- Service configuration
- User accounts
- Password settings
- Audit log settings

Applications that reside on the computer systems might also have their own configuration documents. These should be gathered as well. Finally, network documentation is required for the network segments pertaining to the applications and systems being audited.

Many organizations will have standard configuration documents for role-specific systems. Examples include the configurations for the following:

- Firewalls
- Web servers
- Mail servers
- Domain Name System (DNS) servers

- File Transfer Protocol (FTP) servers

Interviews with Key IT Support and Management Personnel: Identifying and Planning

Interviews play an important role in both the information-gathering process and during the audit. Interviews with IT management, for example, can reveal expectations about the organization to the auditor. Interviewing IT support personnel can reveal pertinent information that might not otherwise be discovered. These interviews can also provide greater focus in areas that need it. For example, those personnel doing the daily work can help identify weak controls and broken processes.

Properly conducted interviews might even reveal more serious violations such as fraud. Effective interviews often result in employees offering information about fraud and other serious activities, even when hotlines and other reporting processes exist. These conversations should be an interview, however, and not an interrogation. A friendly and nonthreatening environment fosters openness and honesty with those being questioned. The Institute of Internal Auditors (IIA) defines the audit interview as “a specialized form of communication used to gain information and assist in evaluation.”

Although interviews play a key role throughout the audit, they help to further define the scope during the planning phase. Individual interviews alone might be reason enough to expand the scope. Interviews looked at collectively can provide the auditor with more information. Taken together, these interviews might reveal patterns. Interviews can aggregate enough data to reveal new information. Reasons to expand the scope from the initial interviews can vary, but common examples include the following:

- Lack of controls
- Override of controls
- Fraudulent activity

Some of the most valuable information for audits will be a result of the interview. Therefore, the interview and how well it is performed can make a difference in the outcome of the audit. A simple framework for conducting effective interviews is composed of the following six steps:

- Preparing
- Scheduling
- Opening
- Conducting
- Closing
- Recording

Preparing for the interview is essential. It is important to be cognizant of others' time and of the job functions they must continue to accomplish even during an ongoing audit. The auditor should prepare a list of questions or at least go into the meeting knowing exactly what it is he or she hopes to achieve or learn. Additionally, an auditor should think like a psychologist. Be aware of the positions and the personalities of those being interviewed. Preparation and scheduling can happen in parallel. It is important, however, to ensure that enough time is given for preparation. When scheduling, the auditor should try to remain as flexible as possible.

The next two steps constitute the actual interview. The opening sets the tone for the remainder of the interview. Opening with a positive tone and clear expectations, combined with thorough preparation, makes conducting the interview much easier. This leads us into

the next step, which is asking the questions. At this point, however, it is not enough to have well-thought-out questions. The auditor must be adept at listening as well. The auditor should understand the reporting hierarchy and how management might influence the interviewee's responses. Closing the interview occurs after the auditor has asked all the required questions or when time is up. The interview should ideally end politely and on an upbeat note. The auditor should thank the interviewee for his or her time and suggest an agreed-upon protocol should the auditor require anything else. This leads into the final step of recording. Taking notes is certainly acceptable during the interview process, but it can be disruptive to the interview flow. Even if notes are taken, after the interview, the auditor should immediately review the notes and organize them as needed.

NIST Standards and Methodologies

NIST 800-53 and NIST 800-53A are two important and widely used standards from NIST. They provide a catalog of security controls and a framework to assess the controls, respectively. As with the ISO/IEC frameworks, many organizations base their policies on NIST. NIST provides many more standards, including low-level documentation that has proven useful for internal auditing and assessments.

The Computer Security Division (CSD) of NIST provides several popular publications. All of their publications reflect their research on IT security issues. The publications they provide include the following:

- **Special Publications**—The 800 series publications, sometimes called **Special Publications**, provide general-interest documents for the IT security community. NIST also publishes the 500 series of Special Publications, which covers IT.
- **NIST Internal Reports (NISTIR)**—The **NIST Internal Reports (NISTIR)** are publications that describe niche technical research.
- **Information Technology Laboratory (ITL) Bulletins**—The **Information Technology Laboratory (ITL) Bulletins** publications provide an in-depth look at timely topics of importance.
- **Federal Information Processing Standards (FIPS)**—The **Federal Information Processing Standards (FIPS)** are standards documents published by NIST and approved by the secretary of commerce.

Of these four different document types, the Special Publications from NIST are more likely to be used for audits and assessments. The publications are known for their depth and prescriptive stance. In addition to the two standards listed at the beginning of this section, the following are examples of other NIST Special Publications:

- SP 800-50, “Building an Information Technology Security Awareness and Training Program”
- SP 800-57, “Recommendation for Key Management”
- SP 800-58, “Security Considerations for Voice Over IP Systems”
- SP 800-61, “Computer Security Incident Handling Guide”
- SP 800-68, “Guide to Securing Microsoft Windows XP Systems for IT Professionals”
- SP 800-70, “National Checklist Program for IT Products—Guidelines for Checklist Users and Developers”
- SP 800-95, “Guide to Secure Web Services”
- SP 800-115, “Technical Guide to Information Security Testing and Assessment”

- SP 800-123, “Guide to General Server Security”

The preceding list provides several examples of the many different publications from NIST. SP 800-70 defines the **National Checklist Program (NCP)**. The NCP is a government repository of available security checklists or baseline configurations for operating systems and applications.

Mapping the IT Security Policy Framework Definitions to the Seven Domains of a Typical IT Infrastructure

The IT security policy framework includes policies, standards, and guidelines. Each of these includes technology, processes, and personnel. The seven domains of a typical IT infrastructure need to be mapped into the framework. The seven domains of a typical IT infrastructure are as follows:

- User Domain
- Workstation Domain
- LAN Domain
- LAN-to-WAN Domain
- WAN Domain
- Remote Access Domain
- System/Application Domain

In some cases, policies might be very specific to only a single domain. For example, the User Domain maps specifically to human resources security. This encompasses controls relating to items such as pre-employment background checks and information security awareness and training. The seven domains also map across various high-level areas. Examples include access control and operations management.

technical TIP

It is helpful to map the infrastructure against the control objectives for the audit. This can provide a clear scope and ensure that every necessary element is addressed against the control objectives. A challenge for auditors is considering the components or pieces of the IT infrastructure that relate to a key issue. Consider the common example of financial reporting. It is not just the application controls that need to be assessed. Even a single financial reporting system may rely on many supporting technologies across the various domains of IT infrastructure. As a result, it is important when developing an audit plan to have a complete picture of all processes and technology across the infrastructure. A security policy framework can help with scope planning by defining boundaries. It also ensures the consideration of all relevant pieces such as interconnected systems to achieve the audit objective. Mapping the security policy framework to the seven domains of IT infrastructure helps define appropriate boundaries for the audit.

Standards further help align the seven domains to the security policy. This includes, for example, access control requirements for networks, users, applications, and operating systems. Just as IT infrastructure needs to be organized within a policy framework, the infrastructure needs to be considered within the framework used for an audit.

The **IT universe** includes all the auditable resources or components within an

organization. Naturally, the seven domains of typical IT infrastructure are a large part of this IT universe. The IT universe may be defined as one or more domains of IT infrastructure or even a portion of a single domain. In addition, the IT universe may describe specific entities, locations, functions, or processes within the organization.

Identifying and Testing Monitoring Requirements

Perhaps one of the most important and beneficial elements of an IT security program for auditors is monitoring. All frameworks include a control objective for regularly assessing and monitoring IT systems and controls. For example, COBIT places a heavy emphasis on monitoring, as defined by the key areas within the framework. COBIT states that continuous monitoring and evaluation of the control environment helps provide answers to the following questions:

- Is IT performance measured to detect problems before it is too late?
- Does management ensure that internal controls are effective and efficient?
- Can IT performance be linked back to business goals?
- Are adequate confidentiality, integrity, and availability controls in place for information security?

Auditors are trying to answer the same questions. Therefore, auditors should identify the tools already put in place by organizations that they can leverage to help answer these questions. Of course, one of the objectives of most audits, regardless of the IT domain being audited, is to identify and test monitoring requirements. Although organizations might have monitoring solutions in place, it doesn't necessarily mean that they are monitoring the right things.

In addition, many companies might be monitoring the right things, but might not have a process in place to make the data actionable. Computer logs provide a perfect example. Are logs being generated? Is the correct information being captured? Is that information being maintained correctly? Are system analysts examining the log data? After analysts examine the data, are any actions taken to deal with identified problems? Depending upon the maturity of the organization, there are many systems that manage these events and information and even provide ways to correlate and make this data more manageable and actionable.

Identifying and testing whether an organization has implemented a sound program for monitoring provides a lot of the information required by an auditor. Consider the following control objectives suggested by COBIT:

- Monitor, evaluate, and assess performance and conformance
- Monitor, evaluate, and assess the system of internal control
- Evaluate and assess compliance with external requirements

The outputs provided from these objectives are a valuable resource to auditors. Except in situations where these controls are nonexistent, auditors can derive usable data regardless of maturity.

Identifying Critical Security Control Points That Must Be Verified

Throughout the IT Infrastructure

Adequate controls should be in place to meet high-level defined control objectives. The organizational risk assessment plays an important role in identifying the high-risk areas. Areas identified as being the most risky should be assessed as often as possible. Levels of risk across the IT infrastructure vary across organizations. This is a result of differing objectives and risk appetites. Regardless, most organizations do share common critical controls.

A great example is the **Consensus Audit Guidelines (CAG)** published by SANS in 2009. These guidelines are now formally known as the Critical Security Controls for Effective Cyber Defense. They include 20 technical control areas deemed critical. These 20 controls, although not prioritized in any order, do establish an overall prioritized baseline of security measures and controls that should be in place at most organizations. This provides not only a baseline from which to identify security controls, but also a way to verify them efficiently and continuously.

NIST Special Publication 800-53, unlike the Critical Security Controls, provides a comprehensive library of security controls. The Critical Security Controls, on the other hand, only provide a subset, but are focused more on what's believed to be the most important controls. Keep in mind that this is only a generalization. After the critical controls are addressed, further controls can be considered from the NIST document, for example.

TIP

The Critical Security Controls for Effective Cyber Defense provide an appendix that maps the top 20 critical security controls to specific controls in NIST SP 800-53.

Building a Project Plan

Having the appropriate people assigned to perform an audit is critical. This affects the effectiveness and efficiency of the audit. Consider that IT professionals could not possibly be experts across all seven domains of the IT infrastructure. Thus, it is not feasible to expect an auditor to be able to perform an adequate audit across all areas. Depending on the scope of an audit, appropriate resources must be obtained to perform the audit.

Other helpful resources include tools to support the IT auditing process. Various tools are available to assist in developing and managing the project plan and associated elements, such as tasks, deliverables, and timelines. The IIA lists several types of tools that can facilitate an audit. These include the following:

- **Electronic work papers**—This provides a document management system to help centralize and provide workflow management of the audit process.
- **Project management software**—This includes mechanisms for managing any project, including auditing projects. These software packages help track progress to established milestones. Project management software is helpful in defining the timeline of the plan and for reporting the status.
- **Flowcharting software**—This provides a way to visually document processes.
- **Open issue tracking software**—This allows for easy tracking of audit deficiencies and areas that still need to be addressed. In many cases, this function can be integrated or included with a document management system.
- **Audit department Web site**—Internal auditing departments typically have an intranet-based solution that provides for collaboration and communication. Even external

auditors benefit from maintaining secure Internet-based portals that provide the same functions.

NOTE

Although resources and budgets can be tight, organizations need to ensure adequate auditing resources. The Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2 states that “an ineffective control environment was a significant deficiency and a strong indicator that a material weakness exists.”

The previous list of tools is useful for the overall management of the audit. During the course of an audit, however, auditors will likely use additional tools to aid in the efficiency and effectiveness of carrying out the audit. Various programs and utilities can help automate tests during the course of the audit. From a planning perspective, it’s important to understand that identification of such tools should be included as part of the planning process.



CHAPTER SUMMARY

Developing an audit plan is a necessary step before conducting the actual audit and reporting findings. Identifying and prioritizing risks is a key component of the audit plan. This provides the necessary information to make informed decisions about the scope and objectives of an audit and what resources will be required. Performing key tasks such as aligning the scope with the objectives and gathering all pertinent information beforehand makes the process of testing controls much easier. The auditor’s ability to conduct the audit and report on the results will be a direct reflection on the approved plan.



KEY CONCEPTS AND TERMS

Audit frequency
Audit objective
Audit scope
Baseline
Chief privacy officer (CPO)
Consensus Audit Guidelines (CAG)
Enterprise risk management (ERM)
Federal Information Processing Standards (FIPS)
Generally Accepted Privacy Principles (GAPP)
Information Technology Laboratory (ITL) Bulletins
ISO/IEC 27005
IT universe
National Checklist Program (NCP)
NIST 800-30
NIST Internal Reports (NISTIR)
Scope creep

Special Publications**Threat****Threat actions****Threat identification****Vulnerability****Vulnerability analysis****CHAPTER 5 ASSESSMENT**

- 1.** Which one of the following can an audit help identify?
 - A. Fraud
 - B. Ineffective IT practices
 - C. Improper use of resources
 - D. Inadequate security
 - E. All of the above
- 2.** Which of the following is the discipline of managing and understanding uncertainty?
 - A. Audit management
 - B. Metrology
 - C. Risk management
 - D. Cryptology
- 3.** Threat is synonymous with risk and can be used interchangeably.
 - A. True
 - B. False
- 4.** Identifying potential dangers to an organization is part of the process called _____ identification.
- 5.** Which of the following is the best example of a potential vulnerability to an IT system?
 - A. Hacker
 - B. Terrorist
 - C. Unpatched operating system
 - D. None of the above
- 6.** The results of a risk assessment help define the audit objectives.
 - A. True
 - B. False
- 7.** When applying controls, which of the following is *not* an example of what needs to be considered when examining the tradeoffs?
 - A. Feasibility
 - B. Cost
 - C. Operational impact
 - D. Due diligence
- 8.** The audit _____ includes the area or areas to be reviewed.
- 9.** Which of the following defines the goals for an audit?
 - A. Audit objective
 - B. Audit scope
 - C. Audit frequency
 - D. Audit report
- 10.** Which of the following is *not* a category of IT security controls defined by NIST?

- A. Physical controls
 - B. Management controls
 - C. Operational controls
 - D. Technical controls
- 11.** Which of the following documents should be included in the gathering process of an IT audit?
- A. Policies and procedures
 - B. Previous audit reports
 - C. Network diagrams
 - D. Answers A and C only
 - E. Answers A, B, and C
- 12.** Only security operations personnel need to follow IT security policies.
- A. True
 - B. False
- 13.** Fraudulent activity uncovered during interviews would be a reason to expand the scope of an audit.
- A. True
 - B. False
- 14.** Which of the following describes all the auditable components within an organization?
- A. Cosmos domains of IT
 - B. Domains of applications
 - C. IT universe
 - D. Universal audit
- 15.** Which one of the following is *not* an example of an audit facilitating tool defined by the IIA?
- A. Project management software
 - B. Flowcharting software
 - C. Electronic work papers
 - D. Presentation software

CHAPTER 6

Conducting an IT Infrastructure Audit for Compliance

A

FTER THE AUDIT TEAM COMPLETES an auditing plan and that plan is approved, the audit team can begin auditing the IT infrastructure for compliance. Testing for compliance is centered on the presence of adequate controls or countermeasures in the planned scope of the IT infrastructure. This includes verifying that policies are put in place and appropriately followed.

The actual execution of an audit can vary widely based on the scope and objectives of the plan. Several methods, frameworks, and automated tools are available to assist in the process. The choices made will depend on the areas being assessed and the depth and breadth at which controls need to be examined.

Chapter 6 Topics

This chapter covers the following topics and concepts:

- What minimum acceptable level of risk and appropriate security baselines are
- How to identify documented policies, standards, procedures and guidelines
- How to conduct an audit in a layered fashion
- How to perform a security assessment for the entire IT infrastructure and individual domains
- How to incorporate the security assessment into the overall audit validating compliance process
- How to use audit tools to organize data capture
- Which automated audit reporting tools and methodologies are available
- How to review configurations and implementations
- How to verify and validate proper configuration and implementation of security controls and countermeasures
- What problems may arise when conducting an IT infrastructure audit
- How to validate security operations and administration roles, responsibilities, and accountabilities throughout the IT infrastructure

Chapter 6 Goals

When you complete this chapter, you will be able to:

- Understand how to conduct an audit of IT infrastructure
- Recognize strategies to manage risk and provide baseline configurations to control risk
- Understand why conducting a gap analysis is important
- Recognize when it is necessary to conduct an audit using a layered approach
- Evaluate different methods and techniques for performing an IT security assessment

- Understand how a security assessment fits into the audit process
- Identify different types of tools used in an audit
- Recognize the value of monitoring and configuration management to the audit process
- Articulate a methodology for testing security controls
- Identify common issues that might hamper the audit efforts
- Understand safeguards necessary for security operations and administration roles

Identifying the Minimum Acceptable Level of Risk and Appropriate Security Baseline Definitions

For an organization to develop security baselines, it must select proper controls. However, the decision to apply or not apply controls is based on risk. Specifically, the controls put in place manage the identified risks. As a result, a risk assessment needs to be completed first.

It might seem easiest to apply a wide range of controls based on different recommendations. Remember, however, that there are costs associated with these controls. For example, you can take many different steps to secure your home and minimize risks. Most people consider door locks as necessary. Beyond that, there is no universal rule of home security to which everyone adheres. Even door locks are available in varying strengths. Consider other measures a homeowner might take. Examples include bars on the windows, storm shutters, insurance, burglar alarms, smoke detectors, carbon monoxide detectors, cameras, safes, watchdogs, outdoor lighting, fences, and even weapons. These examples of home controls are similar to IT controls in that there is a cost associated with each of them. Depending on the type or mission of the business, the cost justifications vary. The controls are based on the level of risk the organization faces.

Payment Card Industry Data Security Standard (PCI DSS) provides an example of a concise set of baseline controls required for those organizations that process or transmit payment card information. The requirements of PCI consider the general risks to payment card data and provide a **baseline approach to safeguarding the sensitive data**. The challenge for many organizations is the need to identify and deal with many different types of risks. This is compounded by a constant shift in threats, vulnerabilities, and changes in technology. The following questions are helpful in determining an **appropriate set of baseline controls**:



WARNING

Effectively managing risks is a complex task. Be careful not to focus only on risk management and lose sight of the organizational goals. If organizations focus more on risk management, they are likely to underperform. You can apply this same principle personally as well.

- Does the organization have a program for IT governance and security management?
- Do IT policies exist?
- Are there tools and processes for assessing risk in place?
- Is the IT environment physically secured?
- Are authentication and access control mechanisms in place?
- Is software to prevent, detect, and respond to malicious code in place?
- Are firewalls used?
- Has a program for configuration and change management been put in place?

- Are systems automatically monitored and reviewed by IT staff?
- Do personnel have the appropriate skills to perform their job, and is an ongoing training and awareness program in place?

Remember that IT is not completely independent. IT exists to support the business. Understanding the minimum level of acceptable risk and implementing baseline controls depend on IT being aligned with the objectives of the business.

Organization-Wide

Establishing a baseline based on a control framework needs to be relative to the **risk appetite** of the organization. The **Committee of Sponsoring Organizations (COSO)** defines risk appetite as “the degree of risk, on a broad based level, that a company or other organization is willing to accept in pursuit of its goals. Management considers the organization’s risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy, and in developing mechanisms to manage the related risks.” Risk appetite is a broad-based look at the amount of risk an organization is willing to take to achieve its objectives. This should not be confused with **risk tolerance**. Risk tolerance is about the ranges of acceptance for specific risks. Identifying levels of risk tolerance allows the organization to stay within its defined appetite for risk.

IT supports the enterprise risk management (**ERM**) strategy in a few ways:

- ERM depends on accurate and timely information. Information systems process and store this information. Maintaining the **integrity and availability** of the data is needed. As a result, adequate controls need to be placed on systems.
- The IT environment supports not only the ERM function but also all other operations of the business. As a result, the IT environment and associated controls need to be aligned with the organization.

In addition to looking at individual controls, an auditor will ensure the IT environment is aligned with the organization’s risk appetite. Additionally, the auditor will assess the framework of internal controls to ensure it is appropriate to allow the organization to remain within its risk tolerances.

Seven Domains of a Typical IT Infrastructure

After considering the organization’s **risk appetite and tolerance**, further consideration of the following is needed:

- The value and importance of data
- Risks to the IT infrastructure
- The level of expected quality of service

NOTE

Most businesses today rely on the Internet as a facilitator for accomplishing their goals. The Internet is a prime example of an IT component that has a clear benefit for the organization, but introduces risk. As a result, basic security controls are applied to protect the organization from numerous threats.

The seven domains of a typical IT infrastructure are composed of people, processes, and technology. This includes employees, partners, and customers interacting with data and using software and applications across a hardware infrastructure. Looking across the seven domains of a typical IT infrastructure can reveal immediate vulnerabilities. For example, domains consisting of remote access, WANs, and cloud computing environments all reveal potential rogue Internet connectivity. Gathering the appropriate documents can provide an immediate view into the domains and inventory of the IT infrastructure.

Mitigating risk within the IT infrastructure includes the application of controls. Again, the risks that organizations want to minimize are based on the value of the assets coupled with how a vulnerability being exploited by a threat would affect the confidentiality, integrity, and availability of the data and associated systems. Reducing the risk depends on what controls are available, how much they cost, and if they are cost efficient. As a result of this analysis, organizations typically take a risk-based approach. A more detailed look at these strategies includes the following:

- **Accept the risk**—Do nothing and manage the consequences if the risk is realized.
- **Avoid the risk**—Seek alternatives or don't participate in the risky activity.
- **Share the risk**—Transfer or divide the risk with other parties.
- **Control the risk**—Apply mechanisms or countermeasures to minimize the effects of the risk.



WARNING

Do not confuse risk acceptance with risk arrogance. Accepting a risk should be a result of careful planning and attention to an assessment of the risk and possible controls or other strategies for managing risk. Risk arrogance or risk blindness occurs when an organization does not adequately assess and plan for risks.

Figure 6-1 provides a simple illustration of components of risk and how the preceding strategies might be applied. The approach an organization takes needs to consider the risk appetite of the organization. The risk might be so great, for example, that avoidance might be the best solution.

In the wake of the attacks on the World Trade Centers in 2001, a reporter asked Bruce Schneier, a security expert, “How can we prevent this from ever happening again?” He replied, “That's easy. Simply ground all the aircraft.” This example of avoiding the risk might seem far fetched, but as Schneier points out, this is exactly what occurred in the hours following the attacks. Although few would argue with the enormous benefits of air travel, the situation at the time merited that an extreme measure be taken.

Consider a simple example of the risk of worms and viruses from the Internet. Think about each of the previous strategies to determine how you might apply each of them to your use of the Internet at home:

- **Accept**—Browse the Web without applying any controls and hope you don't get infected with malicious software. If you do, you will have to deal with the consequences, which might include losing all your data and having to pay expensive repair costs.

Probability

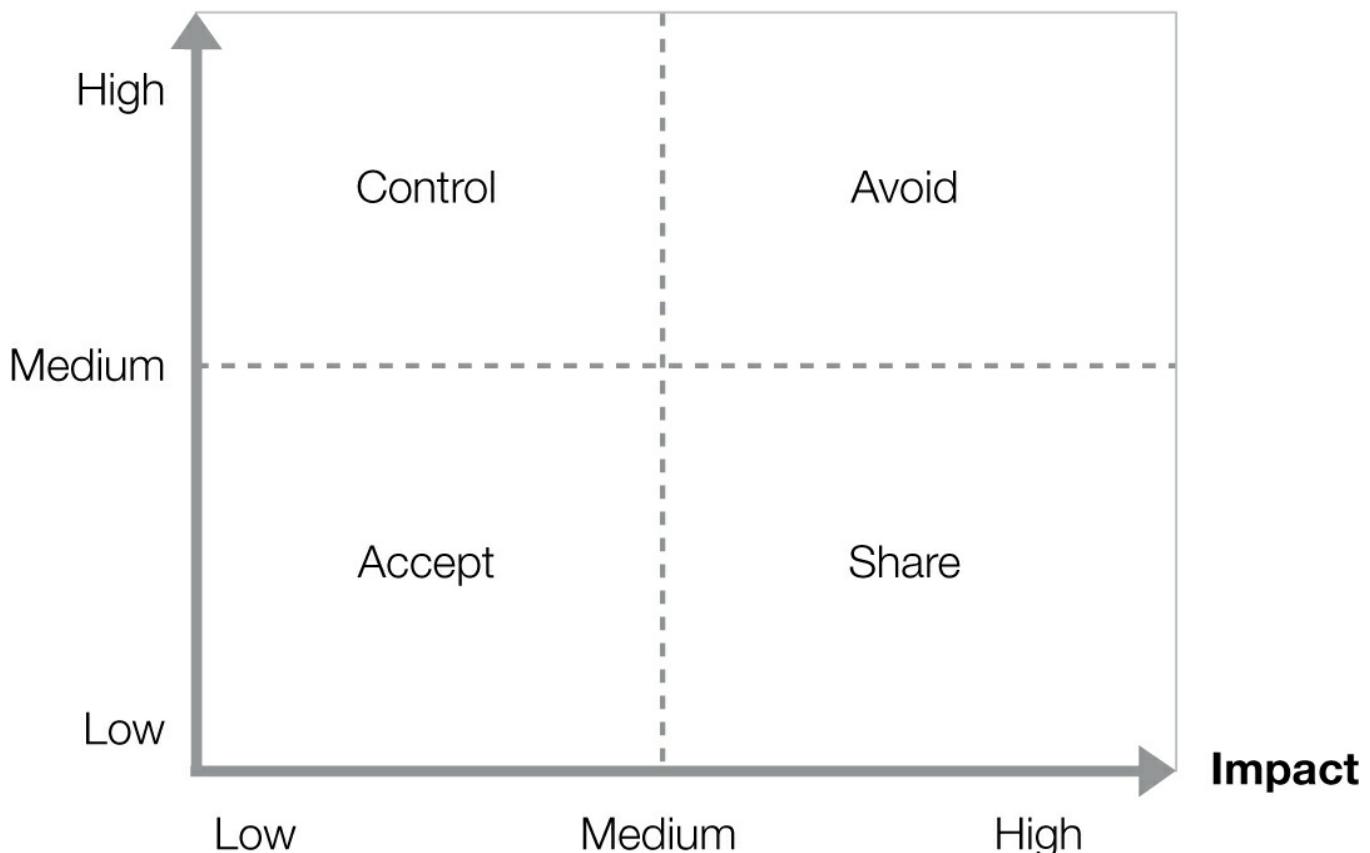


FIGURE 6-1 Applying risk-management strategies.

- **Avoid**—Disconnect your computer from the Internet. You will have certainly eliminated the possibility of being infected with malicious software from the Internet. On the other hand, you no longer receive the benefits of what the connection can provide. But of course, if you used the Internet primarily for research, for example, you can instead use other sources of information, such as books and encyclopedias.
- **Share**—Use the Internet from publicly available Internet kiosks or libraries. Although this might not be as convenient, this does provide a compromise between acceptance and avoidance.
- **Control**—Purchase antivirus software. This option, however, introduces costs. The costs might involve money and degradation of system performance, for example.

Although the preceding example is relatively simple, the decisions are not always so clear. Two additional concepts in selecting an approach include the introduction of new risks and compensating controls. The introduction of new risks is always a possibility when seeking to mitigate risks. Consider the third example from the preceding list. Do you incur a risk that might have otherwise not existed? For example, does driving to the library introduce the likelihood of being involved in an accident?

Compensating controls are alternative measures put in place to mitigate a risk in lieu of implementing a control requirement or best practice. Using the preceding example, suppose you don't want to spend the money on antivirus software and choose to accept the risks. You might take a compensating measure, such as not opening file attachments or only visiting reputable Web sites. Often, layering compensating controls is necessary. In addition to changing your habits, you might also back up your data regularly.

Armed with an understanding of risks within the IT infrastructure, the risk-mitigation

strategies will be factored into the appropriate security baseline. An audit of the **baseline controls** will determine the following:

- Are the controls effective at reducing the targeted risk?
- Do the controls incorporate a mix of preventive, detective, and corrective controls?
- How are the controls monitored and audited in case of failure or breach?

Baseline controls are those countermeasures that apply broadly to the entire IT infrastructure. An exterior door lock on a home is analogous to a common baseline control. Antivirus software is an example of a baseline control within the Workstation Domain. A firewall, which controls access between the organizational network and the public network, is a baseline control for the LAN-to-WAN Domain. In these examples, the controls are configurable depending on the level of risk. Depending on the sensitivity of the data or services, the organization can make further adjustments. For example, does the antivirus software perform periodic scans or does it scan files continuously? A firewall is flexible regarding the level and extent of services it controls. A firewall can place tight restrictions on point-to-point communications or limit what services or applications are able to traverse.

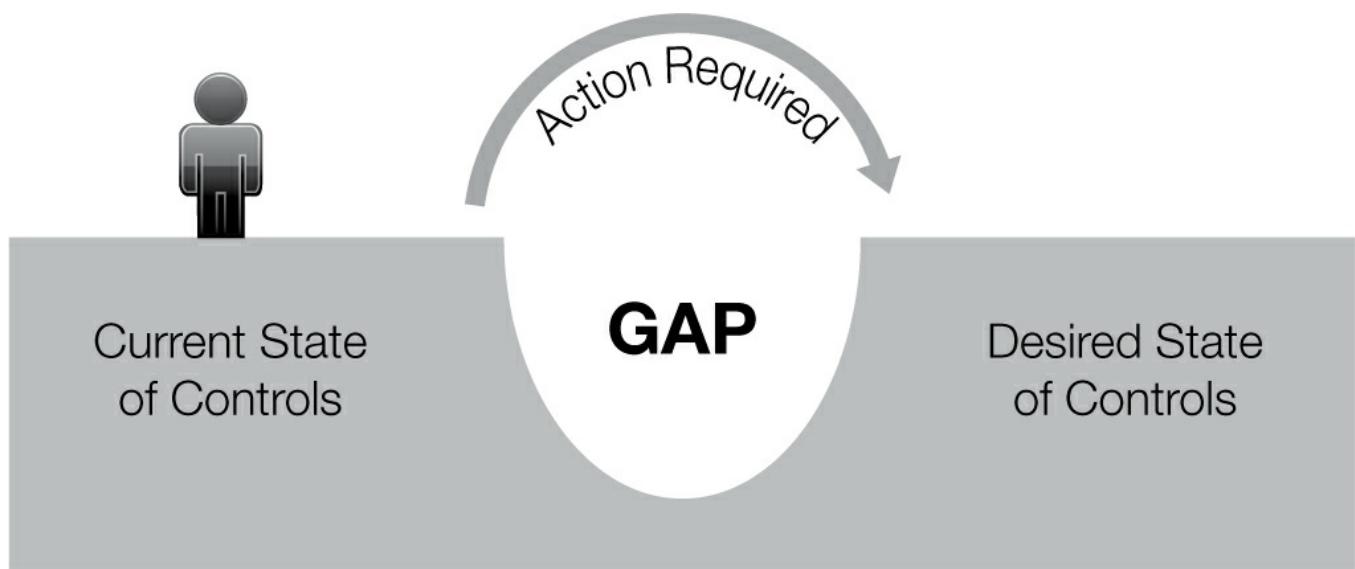


FIGURE 6-2 Control gap analysis.

Gap Analysis for the Seven Domains

A gap analysis is an examination of the current state of controls against the desired state of controls, as illustrated in [Figure 6-2](#). The difference between the two indicates the required action. The ongoing risk-assessment process determines the desired state. Thus, once a gap is closed, it does not necessarily stay that way. The results of a gap analysis determine the absence of baseline controls. Moreover, a gap analysis is ideally used once a baseline is established. It further defines the need for additional controls or enhancements to existing controls.

Analyzing gaps requires attention to the type of system and its value or criticality. Depending on the criticality of the system, different baselines may apply. The National Institute of Standards and Technology (NIST) provides baseline control recommendations across three different types of information systems: low impact, moderate impact, and high impact. NIST provides different baseline controls for different classifications.

Gap Analysis of Service Providers

Many organizations use and continue to expand their use of external service providers for operational, IT, and even IT security functions. The concept of a gap analysis can also be applied to these service providers. First, organizations should assess the security controls of any third party to which they outsource any of their IT or business functions. This might involve verifying the service provider has completed an SOC 1 or SSAE 16 audit. Organizations should also review the specific controls in place at the service provider. It is not unusual to find that a service provider's controls aren't up to the standards of its client organizations.

As a result, organizations can take several approaches. For example, they might decide that the use of the service isn't worth the risk. They might look for another provider that can support the required security controls. Other possibilities include negotiating with the service provider or examining contractual obligations of the service provider. Finally, an organization might employ further compensating controls within the organization if it continues to use the services and if the service provider cannot support the additional controls.

FYI

Multifactor authentication is analogous to using an automatic teller machine. Withdrawing money requires a personal identification number (PIN) and a physical card. Neither component by itself is sufficient. Information systems typically rely on a combination of two or more components for authentication. Typically, this includes something held, such as a card or a token that provides one-time passwords, along with something known, such as a password or PIN. Something inherent might also be included in the authentication process, including biometric features such as a fingerprint.

For example, users accessing low-impact systems might be required to identify themselves with a unique user name and authenticate with a password. This would meet a baseline requirement of an information system uniquely identifying and authenticating users.

Consider an example from NIST 800-53 for monitoring physical access in an information system environment. The control states that the organization should do the following:

- Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents.
- Review physical access logs.
- Coordinate results of reviews and investigations with the organization's incident response capability.

The previous points represent the baseline control for all systems regardless of the impact level. NIST further provides two more control enhancements for monitoring physical access. These are as follows:

- The organization monitors physical intrusion alarms and surveillance equipment.
- The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.

Systems designated as being of a moderate impact would require not only the original baseline control but also the first control from the previous two items. The high-impact system baseline control would require the original baseline control and both controls from the previous list. If an organization had broadly implemented the original baseline controls

but not the others, a gap analysis would reveal whether the control enhancements were necessary. As a result, the organization would clearly understand where it currently stands with regard to monitoring physical access. It would also understand where it needs to be and have clear guidance on what it needs to do to fill the gap.

Identifying All Documented IT Security Policies, Standards, Procedures, and Guidelines

The organizational security policy framework is the foundation for the management of information security. This foundation provides internal direction and support as well as providing direction for assessments and audits. The quality of the entire information security program depends on the policies in place. Fortunately, policies can be one of the least expensive controls. Unfortunately, they are often the most difficult to implement effectively. In fact, the first control objective within the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002 standard states that management should set a clear policy direction by implementing and reviewing the security policy document. The policies provide reference documents for auditors and provide the statement of management intent throughout the organization. As a result, the policy framework, which also includes standards, procedures, and guidelines, will help guide the organization and audits.

Although frameworks such as ISO/IEC 27002 provide guidance for policy development, the scope and maturity of policies vary widely across organizations. It is not uncommon to find companies that lack any type of policy framework at all. Only slightly better are organizations that have a basic or boilerplate policy in place. In these situations, audit and compliance groups are valuable resources to help review the proposed policies, making sure they are realistic, in line with business objectives, and enforceable.

During the audit discovery, the governing policy document should have already been reviewed. During the course of the audit, however, this policy will help identify the standards, procedures, and guidelines needed to effectively understand and assess the IT environment. Although explicit audits against the documented policies and supporting documents are common, the existence and extent of such documentation should always be considered regardless of the type of audit. In other words, the auditor should always identify and evaluate policies, standards, and procedures. Even though ISO/IEC 27002 has a control objective dedicated to security policies, it references individual policies, standards, and procedures throughout all the other controls as well.

The IT infrastructure audit requires the auditor to rely heavily on the documented policy framework. This helps identify the gaps for improvements to the policy as well as fulfill the responsibilities to evaluate adequate controls. Ultimately, the goal is to gain assurance around the strategic view and use of IT controls. Realizing this goal is built on the security policy framework.

Conducting the Audit in a Layered Fashion

The auditor should conduct the audit according to the scope of the plan. This includes auditing the systems included in the plan within the specified time frame. Categorizing the audit into recognizable chunks by domains helps keep the audit focused with minimal reference to other systems. Although the scope may be defined to a specific domain, the auditor needs to recognize the various system inputs, processes, and outputs. This ensures

that other domains are covered as needed.

A layered audit approach across the domains of the IT infrastructure will be necessary when systems span the domains. This is especially evident in audits of a particular process. An external audit over financial reporting controls is a perfect example. A company's financial system can span multiple domains and even include third-party providers such as payroll service providers. This means the auditor has to verify the controls considering the process and the infrastructure that the process uses.

Performing a Security Assessment for the Entire IT Infrastructure and Individual Domains

Various tools are used to perform a security assessment. The assessment may target the entire IT infrastructure, a single domain of the IT infrastructure, or anything in between. All assessments should follow a plan and be performed with a disciplined approach. There are different approaches to identify security weaknesses within an organization. Some of the approaches include the following:

- **Network scan**—This provides an automated method for discovering host systems on a network. Although a **network scan** doesn't necessarily discover all vulnerabilities, it does determine which systems are active on the network and what services they offer or what ports are available. A network scan provides valuable information pertaining to the environment. A network scan can also provide an adversary with a footprint from which he or she can later conduct a more targeted attack. For this reason, network scans are an important part of defining the assessment process and understanding what an attacker might discover and target.
- **Vulnerability scan**—This provides the fundamental process for managing vulnerabilities. A **vulnerability scan** is an automated method for testing a system's services and applications for known security holes. Most vulnerability scans also provide reports on the identified holes along with additional information for improving security. Unlike a network scan, which looks more broadly for available systems, a vulnerability scan is targeted to specific systems. Vulnerability scans can be conducted across the entire infrastructure or specific components within the individual domains, such as the following:
 - Operating systems
 - Web servers
 - Mail servers
 - Databases
 - File Transfer Protocol (FTP) servers
 - Firewalls
 - Load-balancing servers
 - Switches and hubs
 - Wireless access points
- **Penetration test**—A penetration test is most often associated with a security assessment. A penetration test, also known as a pen test, is an active, hands-on assessment that uses methods similar to what a real-world attacker might use. A penetration test goes beyond simply looking for vulnerabilities. When vulnerabilities are identified, a penetration test attempts to actually exploit the vulnerability. The test helps

determine how practical or viable specific attacks might be. This includes understanding what the impact might be of a successful attack.

The technical skill set required to conduct a security assessment depends on the scope of the assessment and the types of tools or techniques used. Knowledge of basic security principles and technical fundamentals, such as understanding **Transmission Control Protocol/Internet Protocol (TCP/IP)**, is helpful. TCP/IP is the basic protocol, or language, of modern networks and the Internet.

All three of the preceding methods may be used independently or may be used together as part of the overall plan. It is common, for example, for a network scan to precede a penetration test. Both network scans and vulnerability scans are more easily automated on a regular basis than a penetration test. Penetration tests require more planning and coordination.

There are several popular frameworks for conducting comprehensive security assessments. Three examples are as follows:

- **Open Source Security Testing Methodology Manual (OSSTMM)**—A method that takes a scientific approach to security testing, the **Open Source Security Testing Methodology Manual (OSSTMM)** is made up of five sections called channels, and each channel includes various modules.
- **Information Systems Security Assessment Framework (ISSAF)**—A method for evaluating networks, systems, and applications, the **Information Systems Security Assessment Framework (ISSAF)** is divided into a three-phase approach, which includes a nine-step assessment process.
- **NIST 800-115**—A guide to the basic technical testing and examination functions of conducting an information security assessment, **NIST 800-115** is composed of seven major sections and several appendixes.

TCP/IP

The language of the Internet and modern networks is the Internet Protocol Suite. This suite of protocols is more formally known as Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is a result of a project of the Department of Defense (DoD) from decades ago. Research and development of the networking protocols continued. By the early 1980s, the DoD had adopted TCP/IP as the standard for its military networks. The 1990s saw the coming of a new application protocol named Hypertext Transfer Protocol (HTTP). This protocol launched what today is known as the Web. HTTP has been mostly implemented on top of TCP/IP. However, HTTP could make use of any reliable protocol. This networking application, along with others such as e-mail, has made TCP/IP the foundation of modern computer networks.

TCP/IP consists of four layers. At the top is the Application Layer. It provides support for the protocols necessary for technology, such as the Web and e-mail, but also for many other different application protocols. Next, the Transport Layer includes several protocols, including TCP. TCP allows communications between applications. The next layer down, the Internet Layer, includes protocols such as IP. This protocol allows communication between computers. Finally, the Data Link Layer is the lowest layer. This layer includes the protocols for the physical and logical network connections used to connect systems on the network.

Protocols within the suite use a numerical identifier or port number to identify how hosts communicate across a network. The port first relies on an **Internet Protocol (IP) address**. The IP address is a numeric label assigned to network systems. The IP address is analogous to your home address. The IP address is a numerical representation to identify and address a system on a network. (As a side note, in the near

future, you will see widespread adoption of a new IP address format to include hexadecimal representation. This new format will fix a current shortage of available addresses.) For each IP address, there are thousands of ports. When a program sends or receives data over a network, the program uses a specific port assigned to a particular IP address. For example, the default port number for communications over the Web is 80. If an IP address is analogous to your home address, a port is the entry or exit point used depending on the situation or application. For example, visitors use the front door, deliveries use the back door, trash is accessed via the side door, cars use the garage door, and a burglar uses an open window.

Regardless of the method chosen, each uses similar techniques for conducting a security assessment. The remainder of this section uses the NIST methodology as a guide. NIST breaks the assessment down across **three different types of primary techniques**:

- Review techniques
- Target identification and analysis techniques
- Target vulnerability validation techniques

Review techniques involve examining the components across the domains of IT infrastructure. Reviewing is a passive process, using noninvasive techniques, which has minimal impact on the systems. **Table 6-1** provides examples of specific review techniques, along with the capabilities of the technique and the specific skill set required to use the technique.

TABLE 6-1 Summary of major capabilities of review techniques.

TECHNIQUE	CAPABILITIES	SKILL SET
Document review	Examines policies and procedures for accuracy and completeness	General knowledge of information security and information policies
Log review	Provides data on system use, changes, and configuration Might reveal potential problems and deviations from policies and standards	Knowledge of log events and ability to interpret log data Ability to use automated logging and log correlation tools
Ruleset review	Exposes holes in security controls based on rulesets	Knowledge of ruleset formats Ability to correlate and analyze rulesets from different devices and different vendors
Network sniffing	Monitors network traffic to capture information such as active systems, operating systems, communication protocols, and services Exposes unencrypted communications	Knowledge of TCP/IP and networking Ability to interpret and analyze network traffic Ability to deploy and use network-sniffing tools
File integrity checking	Identifies changes to important files and can identify unwanted files that might be malicious	General file system knowledge Ability to use file integrity checking tools and interpret the results

After performing a document review, the next step involves the use of target identification and analysis techniques. The goal is to identify active devices along with their available ports and services and look for possible vulnerabilities. The information collected sets the stage for the next step of trying to exploit and validate the vulnerabilities. **Table 6-2** provides examples of the techniques involved, along with the capabilities of the technique and the specific skill set required to use the technique.

TABLE 6-2 Summary of major capabilities of target identification and analysis techniques.

TECHNIQUE	CAPABILITIES	SKILL SET
Network discovery	Discovers active devices on the network Identifies communication paths and facilitates determination of network architectures	General TCP/IP and networking knowledge Ability to use both passive and active network discovery tools
Network port and service identification	Discovers active devices on the network Discovers open ports and associated service/applications	General TCP/IP and networking knowledge Knowledge of ports and protocols Ability to use port-scanning tools Ability to interpret results from tools
Vulnerability scanning	Identifies hosts and open ports Identifies known vulnerabilities Provides advice on mitigating discovered vulnerabilities	General TCP/IP and networking knowledge Knowledge of ports, protocols, services, and vulnerabilities Ability to use automated vulnerability-scanning tools and interpret the results
Wireless scanning	Identifies unauthorized wireless devices on the network Discovers wireless signals outside an organization Detects potential backdoors and other security violations	General knowledge of computing and wireless transmissions, protocols, services, and architecture Ability to use automated wireless scanning and sniffing tools

Finally, with the information from the previous phase, potential vulnerabilities are probed further. The techniques shown in [Table 6-3](#) are used to exploit the vulnerability.

An organization may use all the preceding techniques as part of an overall security assessment or selected parts. Additionally, the techniques can be used across the IT infrastructure or they may focus on only specific domains. This depends on the objectives of the assessment, which must consider available time and resources.



WARNING

The techniques listed in [Table 6-3](#) pose a greater risk during the assessment process than review and target identification and analysis techniques. Although there are benefits to testing and exploiting vulnerabilities in an assessment, these methods could negatively affect the targeted systems. Because this, you should never conduct these techniques without the expressed consent of senior management or risk owners.

TABLE 6-3 Summary of major capabilities of target vulnerability validation techniques.

TECHNIQUE	CAPABILITIES	SKILL SET
Password cracking	Identifies weak passwords and password settings	Knowledge of secure password composition and how operating systems maintain passwords Ability to use automated cracking tools
Penetration testing	Tests security using the same methods and tools that attackers use Verifies vulnerabilities Demonstrates how vulnerabilities can be exploited iteratively to gain access to internal systems	Extensive knowledge of TCP/IP, networking, and operating systems knowledge Advanced knowledge of network and system vulnerabilities and exploits Knowledge of techniques to evade security detection
Social engineering	Allows testing user awareness and if proper procedures are followed	Ability to influence and persuade people Ability to remain calm under pressure

Incorporating the Security Assessment into the Overall Audit Validating Compliance Process

The section “Performing a Security Assessment for the Entire IT Infrastructure and Individual Domains” listed some security assessment techniques. These techniques help determine the feasibility of a successful attack against organizational resources. A security assessment is a component of a full IT security audit. Despite the technically focused nature of security assessment methods such as penetration testing and vulnerability assessments, they are not substitutes for an internal audit of IT security. An audit should also include a risk assessment and pay particular attention to internal controls.

The overall process of validating compliance should take a more holistic view. A penetration test, for example, might reveal only a limited number of vulnerabilities that are actually exploited, thus ignoring other vulnerabilities. As a result, these tools and methods should complement the overall audit process.

ISACA produces a series of auditing standards, guidelines, and procedures for information systems auditors. Its standard titled “Performance of Audit Work” states, “IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met.” The standard further states, “During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives.” These statements justify the use of security assessment techniques such as penetration testing and vulnerability analysis. The security assessment should support the findings within the final audit report.

In fact, the ISACA procedural document “Security Assessment—Penetration Testing and Vulnerability Analysis” provides information system auditors with guidance. ISACA’s suggested penetration test and vulnerability analysis procedures include the following:

- **Planning**—This defines the scope of the evaluation, including objectives, timing, and tools required.
- **Skills required**—This identifies the skills and knowledge required.
- **Agreements**—This provides guidance on the types of records to keep and contractual recommendations if external consultants are involved.
- **Scope questions**—This offers guiding questions regarding the technical scope of the tests to be performed.
- **Internet penetration testing**—This provides recommendations for system enumeration, vulnerability analysis, and vulnerability exploitation from outside the organization.
- **Dial-in penetration testing**—This provides guidance for conducting assessments against dial-in technologies.

FYI

In certain situations, an automated vulnerability assessment tool might be all that is needed to satisfy audit requirements for industry standards. PCI DSS, for example, qualifies companies that offer automated vulnerability assessment tools as approved scanning vendors (ASVs). In some instances, these solutions even offer the ability to automatically submit results to the required parties. This includes the

mergers and acquisitions of banks in the example of PCI DSS.

- **Internal penetration testing**—This provides recommendations for system enumeration, vulnerability analysis, and vulnerability exploitation from within the organization.
- **Physical access controls**—This provides recommendations to gain physical access to the network and procedures to perform after physical access is obtained.
- **Social engineering testing**—This provides guidance for preparing and conducting social engineering attacks.
- **Wireless**—This provides procedures for discovering and exploiting wireless networks.
- **Web application**—This provides procedures for analyzing and attacking Web-based vulnerabilities.
- **Report**—This recommends preparing the final report in accordance with auditing standards and conducting appropriate follow-up activities.

In many situations, an information systems auditor might not have the skills necessary to perform a security assessment. Additionally, there might be other limitations or constraints that prevent the auditor from performing such a technical analysis. In such situations, the auditor might consider using the work of other experts. The expert can be internal or external to the organization as long as independence and objectivity are preserved. Examples of experts provided by ISACA include the following:

- An information system auditor from an external accounting firm
- A management consultant
- An IT expert or expert in the area of audit who has been appointed by top management or by the information systems audit team

The auditor should determine that the expert's work is relevant to the audit objectives. The auditor should also obtain a letter indicating that he or she has the right to access the results from the work of others. Before incorporating the results of an assessment into the audit, the auditor should review all supporting documents and reports. This includes determining that the assessment supports the audit objectives. If necessary, the auditor should conduct additional testing for supporting audit evidence if it is not covered in the assessment.

Using Audit Tools to Organize Data Capture

Auditors can increase their productivity through the use of **computer assisted audit tools and techniques (CAATT)**. These tools and techniques are simply computer applications that auditors use to assist them in their job functions. With these tools, auditors can perform tests that otherwise might be difficult or even impossible to do manually. This includes analyzing large amounts of data or increasing the coverage of the audit.

Although there are many specialized audit-specific tools available, even an office spreadsheet application is considered a CAATT. The tools and techniques include general audit software, audit expert systems, utility software, and even simple queries and scripts. CAATTs are used for many different functions, including the following:



NOTE

Publications and documents sometimes use the acronym CAAT instead of CAATT. In general, the term can describe both tools and techniques. In addition, it is not uncommon to see the acronym use the term *aided* rather than *assisted*.

- Testing transactions in applications
- Reviewing procedures
- Testing system and application controls for compliance
- Conducting automated vulnerability assessments
- Performing penetration testing

During the course of an audit, one of the objectives of the auditor is to produce evidence. Much of the process will still be manual. The use of CAATTs, however, allows for the production of much more evidence than what would be possible manually. Before using an automated or computer-based tool, the auditor should first be familiar with the tool and have the necessary knowledge and skills required to use it. The auditor should also take necessary steps to be successful and to limit the risk of using such tools during the process. Examples include the following:

- Establish any related resource requirements. This includes making sure the needed IT facilities, equipment, data, and personnel are available and accessible.
- Understand the type of data to be examined. This includes how much data, what type of data, and the format of the data.

Using Automated Audit Reporting Tools and Methodologies

Many organizations use automated audit reporting tools. Most systems, for example, are capable of producing many different types of audit logs. These logs detail various types of activity throughout the system, including security data. Examples include the following:

- Failed authentication attempts
- Technical policy changes
- Account changes
- Privileged use

Traditionally, the challenge is managing the voluminous amount of data generated by these systems. This problem is further compounded considering the number and different types of systems across an organization. The components within the seven domains of typical IT infrastructure, for example, are all capable of producing audit trails or log data. Making matters more difficult is the fact that an event generated in one domain may likely contribute to other events being generated in the other domains. Yet by maintaining a silo approach to storing and managing this data, correlation of events is not easy and might be impossible.

Fortunately, automated solutions are available and in use by many organizations. These solutions aggregate all of this data centrally and provide mechanisms to correlate, alert, and report upon this data. These solutions can provide meaningful data from otherwise huge amounts of raw log data. From an organizational perspective, automated audit reporting tools or information and event management help simplify compliance, improve security, and optimize IT operations. Specific examples include the following:

Event Correlation

Event logs can provide valuable information. Fortunately, nearly every type of system is capable of generating log data. Furthermore, some systems can bring all of these disparate logs together into a single location. Unfortunately, this creates a mountain of log data, which can be so overwhelming that eventually it all just gets ignored.

Event correlation enables organizations to better manage the vast amounts of data. Correlation of events provides a more effective means to mitigate threats and vulnerabilities, as well as respond more quickly to incidents. A terminated employee account, for example, can be associated with an attempt to log on to a system with that same account. Individually, this data would not generate any alerts, but when combined, it becomes valuable information. In another example, multiple rules can be tied together. Consider the following example, which would detect a sequence and pattern of activity within the environment indicative of malicious code:

- *If* 10 instances are detected of IP spoofing or denied connections or successful connections without account data to any firewall ...
- *and* you detect 10 instances of resource starvation to any IDS device occurring from the same IP address as the previous rule ...
- *and* this occurs within 60 seconds ...
 - *then* perform some type of action, such as generate a visual alert and send an e-mail to IT security operations staff.

- Meeting compliance regulations requiring the retention and review of audit records
- Identifying security incidents, such as policy violations and fraudulent activity
- Diagnosing and preventing operational problems
- Conducting forensic analysis
- Establishing operational, security, and performance baselines and being able to identify new trends and problems
- Reporting on historical data

Table 6-4 provides a sample set of taxonomy for data collected and associated sample events. Security operations should regularly review the data, from which meaningful information can be abstracted. Additionally, operations should leverage programmatic alerts and correlation rules to help identify suspicious activity.

Audit and logging systems need to be maintained to perform an efficient analysis of events. Whereas a single failed logon, for example, might not be a cause for concern, many rapid failed logon attempts should be. Maintaining and managing audit logs through the use of these systems also provides the organization with a great mechanism to respond to audit requests. This, of course, provides an auditor with a trove of available data to support the evidence-gathering process. Auditors can take, for example, a representative sampling of logs from the various systems across the IT infrastructure to ensure that automatically audited events comply with the stated policies and procedures.

TABLE 6-4 Types of log data and information the data might reveal.

DATA CATEGORY	COMMON EVENTS	SUSPICIOUS ACTIVITIES REVEALED
Computer performance	Resource usage, errors, availability, shutdowns, and restarts	Unauthorized use, compromised systems, denial of service (DoS) attacks
Network performance	Traffic load, errors, network interface status, network scans	DoS and distributed denial of service (DDoS) attacks, information-gathering

		activities as a precursor to actual attack
Users	Logon and logoff data, privilege use and modifications, failed system access attempts	Brute-force attacks on passwords, compromised accounts, privilege abuse
Applications	Application-specific events depending on type, such as Web servers, firewalls, databases, remote access servers, and Domain Name Servers (DNS)	Attempts to exploit vulnerabilities, brute-force attacks, information-gathering activities as a precursor to actual attack, DoS attacks
File system	Access to data, changes to access control lists, changes to file properties, file additions, and file deletions	System compromise, privilege abuse

Reviewing Configurations and Implementations

Managing the configuration of information systems is traditionally a function of IT operations. Configuration management, however, has a direct impact on information security and compliance. As a result, **security configuration management (SCM)** pertains more specifically to the configuration items that are directly related to controls or settings that represent significant risk if not managed properly. This includes the controllable parameters for hardware and software. Configuration management as a program is made up of several pieces, such as the following:

- **Configuration change control board**—A group of personnel responsible for governing configurations and configuration changes
- **Baseline configuration management**—The plan for establishing the basic standard of system configurations and the management of configuration items
- **Configuration change control**—A process for managing changes to the configuration standards defined for information systems
- **Configuration monitoring and auditing**—A process for identifying current configurations and testing configurations against established baselines

The configuration includes the specifics on a system's settings. Auditors can review the implementation of configuration items to ensure that prescriptive controls are put in place. The configuration can then be compared with standards and procedures. This task is difficult, however, in the absence of the previously mentioned components of a configuration management program. Even with a change control process in place, systems undergo unauthorized and untracked changes. These changes can directly affect the security of the systems. In addition to unauthorized changes, monitoring helps identify the following:

- **Misconfigurations**—This ensures that authorized changes are correctly put in place and remain in place.
- **Vulnerabilities**—These include missing system patches as well as configuration items related to a missing patch to determine and prioritize risk.
- **Unauthorized systems and software**—These include systems not managed by a configuration monitoring solution as well as software not authorized for use on the managed system.

What makes configuration management especially useful for auditors is that most of the data about the systems is contained in a **configuration management database (CMDB)**. The CMDB provides a central repository from which reports can be run. Thus, everything about all the

systems at a particular point in time is stored in a database. Examples of configuration items include the following:

- Operating system type
- Service pack level
- Security patches
- Software installed
- Users
- Device drivers
- Hardware configuration
- Service and port status
- Access permissions
- Authentication controls
- Audit settings
- Protocols

Many configuration monitoring and auditing solutions are capable of providing predefined templates from which the configuration items can be assessed. Many of these templates are based on industry-recommended practices such as those from NIST. In addition, organizations can configure auditing templates to align with their own internal policies and standards. The following are sample templates that can be programmatically run to assess parameters specific to the template:

- **Operating system**—This includes audit templates for each version of the operating system across UNIX, Linux, Mac OS, and Windows, for example.
- **Database**—This includes audit templates for different types of databases that verify the database security and configuration parameters.
- **Application**—This includes audit templates to assess applications for expected configurations.
- **Network device**—This includes templates to verify appropriate settings across the network infrastructure, such as routers, switches, and firewalls.
- **Best practice documents**—This includes templates to be run across different parts of the infrastructure to test for compliance based on recommended practices from organizations such as NIST and the Center for Internet Security (CIS).
- **Regulations and standards**—This includes templates specifically targeted to assess against regulations such as the Health Insurance Portability and Accountability Act (HIPAA) or industry standards like PCI DSS.

When systems aren't compared against acceptable baselines, the systems could be configured inconsistently in a number of different ways. Configuration management and the use of monitoring tools ensure that systems stay configured as originally intended. This makes systems easier to troubleshoot and maintain and makes them more secure.

Verifying and Validating Proper Configuration and the Implementation of Security Controls and Countermeasures

Auditing security controls across the IT infrastructure involves testing the controls or

countermeasures using available documents, interviews, and personal observation.

This section provides an overview of testing and validating controls based upon NIST SP800-53A, which provides an approach to assessing security controls. Regardless of the exact methods used, however, the principles are the same.

Each control to be tested should have an accompanying assessment objective. The objective provides the foundation or high-level statement to determine the effectiveness of the control. Based on this, one or more assessment objectives are validated using a specific method. Such methods include examination, interviews, and testing. Using these methods against particular assessment objects will produce the results, which is a determination of the effectiveness of the controls. The assessment objects vary and include different types of elements. Three broad categories of objects include the following:

- **Specification objects**—These include documents such as policies, procedures, plans, and architectural designs.
- **Mechanism objects**—These are the specific hardware and software countermeasures installed and configured.
- **Activity objects**—These are the security-related actions involving IT personnel.

The effort required to assess controls will vary not just across the objectives. The auditor should also consider impact levels, or the sensitivity and importance of the information systems. The effort is directly related to the depth and breadth of the assessment. NIST's assessment framework uses the terms depth and coverage and also defines their associated values. A summary of these definitions is as follows:

- **Depth**—This addresses the thoroughness and level of detail in the examination, interview, and testing process.
- **Coverage**—This addresses the breadth of the examination, interview, and testing process of objects.

Depth and coverage each have three different values. The values that address depth are generalized, focused, or detailed. The values that address coverage are representative, specific, and comprehensive. Representative coverage makes use of a limited sample of assessment objects. Further, the goal is to determine that a security control is put in place and that there aren't obvious faults. More specific coverage builds on this by increasing the scope to achieve greater confidence that the control is not only put in place correctly with no obvious faults, but also operating as intended. Finally, comprehensive coverage uses a much larger sample of assessment objects to achieve the results of representative and specific coverage. It also ensures the control is operating on an ongoing basis that is continually improved.

The varying levels of depth have the same relative expectations. This includes making sure controls are put in place and free of obvious errors. It also includes making sure the controls are consistently operating as intended and are supported by continual improvement. Interviews and document reviews at a general level include high-level discussions and examination. A more focused assessment asks questions in greater depth and requires a more detailed analysis of documents. Finally, a detailed assessment includes asking deep, probing questions and performing thorough analysis of documents across a greater body of evidence.

In addition to interviews and document reviews, testing depth uses methodologies that require varying degrees of knowledge about the environment being tested. This ranges from having no knowledge of the infrastructure or implementation of a control to having

considerable and extensive knowledge of both the infrastructure and details about the control.

Based on the tests of each control, an unbiased and factual determination is made as to the effectiveness of the control. The control should either satisfy or not satisfy the expected state. In some situations, the auditor will not be able to determine how effective a control is because of lack of information or an inability to test. In situations where the objectives of the control are not fulfilled, the auditor needs to understand and document how the control differs from what is expected. In addition, the auditor should note how these findings affect confidentiality, integrity, and availability.

Black, White, and Gray Boxes

Testing systems requiring varying degrees of knowledge about the overall infrastructure and control are often classified as black box, white box, and gray box. This terminology is frequently used when conducting penetration tests, software tests, and tests of controls or countermeasures.

Black-box testing assumes no knowledge of the inner workings of a system. The idea is that no one can see inside of the box. White-box testing assumes complete and explicit knowledge of everything about the system. This explains why white-box testing is also known as glass-box or clear-box testing. It provides visibility or transparency. Finally, gray-box testing, as the name suggests, is somewhere in between a black-box testing and white-box testing. A gray-box test is more appropriately described as a translucent box.

When testing the adequacy of controls, the type of testing the auditor conducts is based on depth. The three attributes of depth are related to these different boxes. Generalized testing is also known as black-box testing. Focused testing is also known as gray-box testing. Detailed testing is also known as white-box testing.

Identifying Common Problems When Conducting an IT Infrastructure Audit

An audit of an IT infrastructure should address the objectives stated within the plan. It should also comply with laws and professional standards of auditing. The audit seeks to discover evidence from which a conclusion can be made. This conclusion is based on the analysis and interpretation of the evidence. Despite the best plans and intentions, however, problems can occur and things can go wrong.

To prevent problems from occurring, the auditors must start with the plan. Having unclear expectations is a common problem with many audits but is easily addressable. The appropriate parties should clearly understand three key points. First, they should understand why the audit is being conducted. Second, they should understand what the scope and objectives are. Finally, they should understand what happens upon completion of the audit.

In addition, interviews and interactions with IT staff are critical throughout the entire audit. Auditors should be careful not to neglect the concerns of the people within the organization. This occurs when auditors are focused entirely on the technology and the gathering of quantifiable data.

NIST defines several areas of potential challenges when conducting security testing and assessments. All these areas could potentially apply to an audit as well. These areas include the following:

- **Time and resources**—A solid plan is critical to maximizing the use of available time and

resources. Both are sometimes underestimated for many different reasons. For example, systems might not be able to be tested during normal business hours. Often, there is only a small window of opportunity each day. Because technology evolves so quickly, assessors and auditors might find that they don't have the requisite skill set to adequately perform specific actions.

- **Resistance**—IT personnel might be resistant to an assessment or an audit for many reasons. Operationally, IT personnel might have concerns about outages. On a personal level, individuals might be defensive and fearful for their jobs or fearful of being reprimanded.
- **Temporary behavior**—Users and operators might adjust the processes and systems for which they are responsible before an audit or an assessment to comply with policies. Upon completion of the audit, however, systems and behaviors often return to the state prior to the audit or assessment.
- **Immediate response**—As weaknesses or audit deficiencies are uncovered, there might be a desire to immediately address the issue. Although generally acceptable and encouraged, changes need to adhere to the organization's policies and change-management procedures.
- **Changing technology**—Technology and the tools used to assess it are constantly evolving. As a result, auditors need to be committed to ongoing information technology education, including the use of new tools and techniques.
- **Operational impact**—There is always the possibility that tests might inadvertently disrupt the systems being tested. To limit any negative impact, the assessor or auditor should maintain proper documentation, including a detailed list of actions being performed.

Validating Security Operations and Administration Roles, Responsibilities, and Accountabilities Throughout the IT Infrastructure

There are many different roles for security operations and administration across the IT infrastructure. Security operations and administration are responsible for implementing the policy framework to protect the confidentiality, integrity, and availability of the company's information and supporting technologies. The foundation of these operations is first based on assigning, identifying, and classifying the information and information systems, and then implementing and maintaining the appropriate controls to protect the information and infrastructure.

NOTE

Security operations and administration personnel need to be held accountable for their responsibilities. Because of the important responsibilities of the security and administration staff, additional safeguards need to be in place to prevent inappropriate use and misconduct.

The tasks include managing authentication and access controls, security hardware, and security software. Security operations and administration personnel are directly involved in the implementation and administration of controls designed to allow access only to those authorized. They also maintain the systems that prevent fraud, violations, and other malicious and even unintentional breaches of confidentiality, integrity, and availability.

Those assigned to protect assets are not above committing irregular or illegal acts. In fact, without proper controls in place, such activities are easier to perform. This includes fraud, theft, suppression of information, and other legal violations. Examples of safeguards that need to be verified include the following:

- **Security operation policies**—Policies form the foundation for holding staff accountable. Policies define the behaviors that must be complied with by security and administration personnel. Periodically testing the staff on the organization's policies helps increase accountability.
- **Assignment of responsibilities**—Those assigned with security and administration roles need to have clear expectations and responsibilities. This helps foster and enforce accountability within the individual roles.
- **Maintenance procedures**—These provide clear guidance for the security operations and administration staff in the performance of their duties to prevent misconfigurations and errors.
- **Segregation of duties**—Segregation of duties divides roles and responsibilities so a single individual or group can't undermine a critical process. From an IT perspective, this includes, for example, separating testing, development, and production environments to prevent unauthorized changes. Another example includes preventing the person who approves configuration changes from being the person who implements them. Segregation of duties is also referred to as *separation of duties* or *separation of responsibilities*.
- **Rotation of duties**—The safeguard of **rotation of duties** rotates employees into different functions and helps mitigate collusion to circumvent what segregation of duties helps prevent.
- **Least privilege**—The safeguard of **least privilege** involves users having access only to what they need to perform their duties.
- **Mandatory vacation**—For sensitive positions, a contiguous one-week vacation should be required. This reduces the opportunity for an employee to commit unethical or illegal acts. It allows others to fill in to support the position and verify the work being performed.
- **Screening**—Employees responsible for managing security and sensitive data within an organization should be carefully screened prior to employment. This includes background checks, for example, to ensure the individuals are suited for the position.
- **Training and awareness**—A continuous program of training is necessary to ensure employees understand the responsibilities associated with their duties and are adequately prepared to perform them effectively.

Security operations and administration personnel need to be held accountable. Strong accountability also serves the goal of preventing fraud and inappropriate use.



CHAPTER SUMMARY

Conducting an IT infrastructure audit for compliance first depends upon an adequate plan. Establishing baselines and identifying an acceptable level of risk across the environment provide a starting point for the actual audit. From there, the audit can follow common methodologies while being flexible based on the expanse of the audit. In addition

to the documents gathered during the discovery phase, the auditor should continue to gather and use available resources during the audit. This includes continued interaction with the organization, the use of computerized audit tools, and the review of available configuration information and audit logs. Upon completion of the audit testing, a final report should be prepared.



KEY CONCEPTS AND TERMS

Baseline controls

Computer assisted audit tools and techniques (CAATT)

Configuration management database (CMDB)

Information Systems Security Assessment Framework (ISSAF)

Internet Protocol (IP) address

Least privilege

Network scan

NIST 800-115

Open Source Security Testing Methodology Manual (OSSTMM)

Risk appetite

Risk arrogance

Risk tolerance

Rotation of duties

Security configuration management (SCM)

Transmission Control Protocol/Internet Protocol (TCP/IP)

Vulnerability scan



CHAPTER 6 ASSESSMENT

1. The decision to apply or not apply controls is based on risk.
 - A. True
 - B. False
2. Which one of the following is the best example of avoiding risk?
 - A. The IT department decides to install an antivirus device at its network border.
 - B. The IT department outsources its vulnerability management program to a third party.
 - C. The IT department disables the ability for end users to use portable storage devices.
 - D. The IT department installs data loss prevention software on all end users' workstations.
3. Which of the following is an examination of the current state of controls against the desired state of controls?
 - A. Control objective
 - B. Gap analysis
 - C. Baseline analysis
 - D. Log review
4. The purpose of a network scan is to identify as many vulnerabilities as possible.
 - A. True

- B. False
5. A _____ is an assessment method that uses methods similar to what a real-world attacker might use.
6. Which one of the following is *not* an example of a review technique?
- A. Password cracking
 - B. File integrity checking
 - C. Log review
 - D. Network sniffing
7. If required, an auditor is justified in the use of security assessment techniques such as penetration testing and vulnerability analysis and may consider using the work of other experts.
- A. True
 - B. False
8. What does CAATT stand for?
- A. Computer Assisted Audit Tools and Techniques
 - B. Computer Aided Assessment Tools and Techniques
 - C. Compliance Auditing Assisted Tactical Techniques
 - D. Compliance Assisted Audit Tactical Tools
9. Which of the following are examples of information provided by audit logs?
- A. Failed authentication attempts
 - B. Account changes
 - C. Privileged use
 - D. All of the above
10. Which of the following benefits does an automated security information and event management log solution provide?
- A. Diagnosing and preventing operational problems
 - B. Assigning appropriate responsibilities to security operations
 - C. Management of a configuration change control board
 - D. All of the above
11. A configuration _____ database provides a central repository of configuration items.
12. Which one of the following best describes an assessment objective for a control?
- A. A high-level statement to determine the effectiveness of a control
 - B. A detailed statement on what activities need to occur to implement a control
 - C. A definition of responsibilities to be assigned to security operations for the management of a control
 - D. A statement about the required depth or coverage required to test a control
13. Which one of the following is *not* an example of a level of depth required to assess a control?
- A. Comprehensive
 - B. Generalized
 - C. Focused
 - D. Detailed
14. Which of the following best describes documents such as policies, procedures, plans, and architectural designs?
- A. Specification objects
 - B. Mechanism objects
 - C. Activity objects
 - D. Configuration objects
15. Preventing a user who approves a configuration change from being the person who implements the change is an example of which of the following?

- A. Rotation of duties
- B. Least privilege
- C. Segregation of duties
- D. Dual control

CHAPTER 7

Writing the IT Infrastructure Audit Report

AFTER DOING AN AUDIT, the final report is arguably the most important part of the process. The report provides the means of communicating the results of the audit. This effectively drives management to consider resources and appropriate steps to improve compliance across the IT infrastructure. The primary purposes of the audit report include the following:

- Communicating the results
- Preventing misunderstanding of the results
- Facilitating follow-up corrective actions

Various entities and standards provide guidance on what should be included in the final report. These include, for example, the following:

- The American Institute of Certified Public Accountants (AICPA)
- The Institute for Internal Auditors (IIA)
- ISACA

The contents of the report will be influenced by the scope, objectives, methods, work performed, use of others' work, and findings. Each of these items forms the basis of most reports. Other items may appear in the final report. These include a statement as to the independence of the report (if required), disclaimers, visual representations, restrictions, concerns, and audit opinions. Audit opinions generally are either unqualified or qualified. In short, an unqualified opinion means the auditor found no discovered exceptions, while qualified means the auditor notes one or more conditional exceptions were found.

Chapter 7 Topics

This chapter covers the following topics and concepts:

- How to write the executive summary of an audit report
- What a summary of findings comprises
- What the IT security assessment results include
- How to report on the implementation of IT security controls and countermeasures
- How to analyze gaps in IT security controls and countermeasures
- How to assess compliance throughout the IT infrastructure
- What to include in compliance recommendations

Chapter 7 Goals

When you complete this chapter, you will be able to:

- Write a proper executive summary
- Understand audit findings and their importance to the audit report
- Understand the gap analysis and its importance to the audit report
- Identify the risk components part of an IT security assessment and audit report
- Understand how IT security controls identified in the IT audit report relate to the security policy framework and protection of privacy data
- Identify key areas from which a gap analysis should be documented
- Understand how to report on a compliance assessment
- Understand how to craft meaningful compliance recommendations

Executive Summary of an Audit Report

A final audit report is usually lengthy. In fact, it may be a combination of several different reports. The report contains detailed issues, findings, and action plans. The **executive summary** provides a brief review intended for senior management or other decision makers. Many executives do not have time to read the full report. Other executives might not have the technical expertise to understand it. The executive summary provides the necessary information for both types of executives.

technical TIP

Unlike introductory text, an executive summary must be able to exist on its own. Many executive summaries are standalone documents and may even have an accompanying presentation.

Unlike typical summaries, the executive summary should be bold and powerful. It should not be vague. It should include pertinent and valuable information. For example, it would not be suitable to provide a finding that states, “Important baseline controls were missing.” Rather, it is better to state, “Over two dozen instances of malicious code were found on systems. And 65 percent of all systems did not have antivirus software installed or enabled.” Although it isn’t necessary to highlight every issue, the executive summary should include or clearly outline the most important issues.

An executive summary can be a single page in length or multiple pages. A good guideline is that the length of the executive summary should be about 10 percent of the final report. For example, a 1-page executive summary is adequate for a 10-page report. A 100-page report may have a 10-page executive summary.

The components typically found in the final report as well as the **executive summary** include the following:

- Introduction
- Objective and scope
- Methodology
- Findings
- Recommendations
- Action plan

All of these are covered in detail within the final report. The final format of the report and executive summary vary by organization. Most important to the executive summary is the review of major issues and findings. This includes making sure to effectively communicate the key issues. This will lead to positive changes within the organization.

Summary of Findings

An audit **finding** is a documented conclusion. It involves deficiencies, abuse, fraud, or other illegal acts. The objective of the audit determines how findings need to be documented. As findings are discovered, further investigation might be required to satisfy the objectives, which will be summarized in the final report. The following four elements constitute a finding:

- **Criteria**—This identifies the expected or desired state. This provides the context for evaluating the evidence collected by the auditor and the subsequent procedures the auditor performs. The criteria might be based, for example, on regulations, policies, standards, and external frameworks.
- **Circumstance**—This identifies the situation within the IT environment that exists.
- **Cause**—This identifies the reason for the gap between the circumstance and the criteria. The cause also provides a starting point from which the auditor can make a recommendation to correct the situation.
- **Impact**—This identifies the effect or potential impact on the IT landscape based on the difference between the circumstance and the desired state. Essentially, this includes consequences that might occur as a result of this difference. It might also reveal negative consequences that have already been occurring.

Within each of the different areas of IT, audit findings can get very specific. A summary of findings across the seven domains of a typical IT infrastructure should be broader. To provide this in a meaningful, yet concise way requires an analysis of the gaps. This includes a measure of where the organization is and where it would like to be. This requires a complete understanding of the systems across the IT domains, as well as the level of control the enterprise needs. Factors that affect the level of control may include regulatory requirements and risk analysis. An auditor might also compare the organization with industry peers and the organization's practices with other recommended practices.

Maturity modeling provides an excellent tool for evaluating an organization and identifying gaps. (*Gap* describes the difference between the current state of the organization versus where the organization should be.) The Control Objectives for Information and Related Technology (COBIT) framework provides a maturity model in the **Process Capability Model**. This model first provides the framework for measuring the performance of a given process. Next, based on the results, it identifies areas for improvement. The maturity of the process is graded on a scale of 0 to 5. A level of 0 means the process is not in place. A level of 5 means the process is continually being improved. Each level also contains one or two attributes. These attributes are used to help define the level at which a process belongs. [Table 7-1](#) provides a summary of each level and its associated attributes.

NOTE

The COBIT Process Capability Model is based on a process assessment approach defined in ISO/IEC 15504.

TABLE 7-1 COBIT Process Capability Model based on ISO/IEC 15504.

LEVEL	DESCRIPTION	ATTRIBUTES	SUMMARY
0	Incomplete process		The process is not implemented or fails to achieve its purpose.
1	Performed process	Process performance	The implemented process achieves its purpose.
2	Managed process	Performance management Work product management	The process is now implemented in a managed fashion and its work products are appropriately established, controlled, and maintained.
3	Established process	Process definition Process deployment	The process is now implemented using a defined process that is capable of achieving its process outcomes.
4	Predictable process	Process management Process control	The process now operates within defined limits to achieve its process outcomes.
5	Optimizing process	Process innovation Process optimization	The process is continuously improved to meet relevant current and projected business goals.

IT Security Assessment Results: Risk, Threats, and Vulnerabilities

A complete security assessment should include details about risk as part of the report. This includes full documentation of the identified threats, vulnerabilities, and resulting risks. The findings inform management of the resulting risk to the environment. This information provides management with the data necessary to make informed decisions to manage risk. The results will help drive how resources are allocated to address potential uncertainties.

The key components of the assessment should include the following:

- **Introduction**—This provides the purpose and scope of the assessment. This includes the systems, personnel, locations, and other details about the assessed environment.
- **Approach**—This describes the methods taken. This includes those involved as part of the assessment and the techniques and tools used to collect information. A description of the risk scale or matrix used should also be discussed.
- **System characterization**—This provides details about the infrastructure systems. This includes the hardware, software, data, interfaces, and associated users. A discussion of existing technical, management, and operational controls may be included.
- **Threat statement**—This is a complete outline of potential threat sources and associated activities.
- **Assessment results**—This provides details on vulnerabilities and threats—specifically, the pairing of threats with vulnerabilities that can be exploited.
- **Summary**—This provides a concise review of the observations as well as risk levels. This may include any recommendations.

The report should describe the approach in detail. This includes the methodology used and details about the approach and definitions. A good practice is to use an established approach to assessing risks. [Table 7-2](#), [Table 7-3](#), [Table 7-4](#), and [Table 7-5](#) are adapted from NIST SP 800-30, “Risk Management Guide for Information Technology Systems.” The final report should include a similar statement with accompanying background on the methodology.

Table 7-2 provides the definitions for determining the likelihood of a threat. The report should then describe the next step to determine the impact that would result from a vulnerability being exploited. [Table 7-3](#) provides the impact levels and associated definitions. Next, the report should provide a determination of the resulting risk. The resulting risk is based on the threat likelihood and the impact the threat would have if successful. [Table 7-4](#) provides the method to determine risk. It is based on multiplying the likelihood of a threat occurring by the impact the threat might have.

TABLE 7-2 Likelihood determination ratings and descriptions.

LIKELIHOOD LEVEL	WEIGHT FACTOR	DESCRIPTION
High	1.0	The threat source is highly motivated and sufficiently capable and controls to prevent the vulnerability from being exercised are ineffective.
Medium	0.5	The threat source is motivated and capable but controls are in place that may impede successful exercise of the vulnerability.
Low	0.1	The threat source lacks motivation or capability or controls are in place to prevent or at least significantly impede the vulnerability from being exercised.

TABLE 7-3 Impact levels and descriptions.

MAGNITUDE OF IMPACT	WEIGHT FACTOR	IMPACT DESCRIPTION
High	100	Exercise of the vulnerability may result in the highly costly loss of major tangible assets or resources. Exercise of the vulnerability may significantly violate, harm, or impede an entity's mission, reputation, or interest. Exercise of the vulnerability may result in human death or serious injury.
Medium	50	Exercise of the vulnerability may result in the costly loss of tangible assets or resources. Exercise of the vulnerability may violate, harm, or impede an entity's mission, reputation, or interest. Exercise of the vulnerability may result in human injury.
Low	10	Exercise of the vulnerability may result in the loss of some tangible assets or resources. Exercise of the vulnerability may noticeably affect an entity's mission, reputation, or interest.

TABLE 7-4 Resulting risks as a product of impact and threat likelihood.

THREAT LIKELIHOOD	IMPACT LEVEL		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	Medium $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

TABLE 7-5 Risk level descriptions.

RISK LEVEL	RISK DESCRIPTION
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, management must determine whether corrective actions are still required or decide to accept the risk.

The resulting product of threat likelihood multiplied by the impact level provides a rating of risk. In this example, it would be categorized as Low, Medium, or High. [Table 7-5](#) provides the description of the resulting rating. This also includes actions that must be taken as a result.

The results of the assessment should include a pairing of identified vulnerabilities with associated threats. For each pair, the report includes a brief description of the threat and vulnerability. It should also give a description of existing controls in place to reduce the risk. The results from the previous tables should also be included as summary items. This includes the threat likelihood rating, risk impact rating, and overall risk rating.

The following is an example of a vulnerability/threat pair analysis: “Weak passwords are vulnerable to hackers.” These passwords are more easily guessed or cracked by automated programs. The existing control enforces passwords to be alphanumeric and at least five characters long. The likelihood, impact, and risk rating are all medium. As a result of the risk, a recommended control such as increasing password complexity or length should be documented.

Reporting on Implementation of IT Security Controls and Countermeasures

To identify and report on security controls implemented, a process needs to be in place to collect and manage this information. Many different types of electronic solutions are available to assist with the process, as well as various examples of control assessment reports. A useful form from the National Institute of Standards and Technology (NIST) is one example. The

form can help you organize information related to security controls and countermeasures throughout the IT infrastructure.

This NIST sample form is composed of the following four sections:

- **Section I: “Information Systems and Assessment Information”**—This includes fields for the name of the information system, assessment dates, impact level, sites assessed, and components where security controls are employed. The components would include infrastructure such as firewalls, routers, and workstations.
- **Section II: “Security Control Information”**—This includes a field for the description of the security control as well as a field for guidance.
- **Section III: “Assessment Findings”**—This includes fields to identify the specific assessment objective, additional determination statements, as well as the assessment methods and objects. Each determination statement provides a column to indicate if the finding was satisfied or other than satisfied.
- **Section IV: “Assessor Comments and Recommendations”**—This includes fields for assessor comments and recommendations. The comments clarify identified weaknesses or deficiencies. Added recommendations can suggest how to correct or improve the implemented security control.

Per Documented IT Security Policy Framework

Are controls put in place as stated in the IT security policy framework? Control frameworks such as those from COBIT, NIST, and the International Organization for Standardization (ISO) are useful here. They provide an effective means to assess and document an organization’s implementation of controls. This process is quite effective, especially when the organization’s framework is based on a well-known external framework.

The organization might have mappings of its controls to well-known frameworks. If available, auditors may use these mappings but should verify them first. This should be included in the final report. In addition, it provides the method for conducting the analysis of any gaps. These gaps should also be documented. Documenting the gap analysis is discussed in the next section.

Privacy Data

Frameworks mentioned earlier include controls. These controls are essential to protecting privacy data. An audit may be concerned with assessing the protection of privacy data. Alternatively, it may be concerned with compliance with privacy laws. In both cases, the audit should report specifically on established privacy principles. Refer to the Generally Accepted Privacy Principles (GAPP) if necessary. Also noteworthy are the organization’s current implementation, related controls, and associated risks. [Table 7-6](#) provides examples of related risks relevant to each privacy principle.

TABLE 7-6 Generally Accepted Privacy Principles and associated risks.

PRIVACY PRINCIPLE	RISK
Management	Lack of accountability can result in inadequate privacy protection as well as noncompliance with legislation.
Notice	If an individual cannot obtain the privacy policies, he or she may deny consent to use personal information.
Choice and	If consent is not obtained prior to collecting personal information, the organization can

consent	suffer reputational risk and loss of customer trust.
Collection	Collecting more information than is needed can result in increased retention and security costs and introduces additional liability.
Use and retention	Personal information could be prematurely destroyed, resulting in information not being available to make important decisions.
Access	Individuals unable to access their information might not be able to correct inaccurate information. This could result in a negative decision being made about the individual, resulting in legal liability.
Disclosure to third parties	Providing data to third parties with inadequate controls could affect customer retention and result in identity theft.
Security for privacy	Inadequate security controls could result in the unauthorized use of privacy data, causing harm to the individual.
Quality	Basing business decisions on inaccurate personal information could result in lost profits.
Monitoring and enforcement	Customer satisfaction and retention might be jeopardized if customer inquiries or complaints are not adequately addressed as a result of an ineffective monitoring process.

The risks to the organization for each of the privacy principles should be clearly documented in the audit report. In recent years, IT security personnel have had to be more aware of privacy implications. The implications are due to the growing number of privacy regulations. IT controls for privacy go beyond just securing data to prevent improper use. Most IT frameworks address privacy to a certain extent. In addition, both the IIA and ISACA publish guidelines. These guidelines establish common privacy controls and audit processes.

IT Security Controls and Countermeasure Gap Analysis

A gap analysis means comparing the “as is” to the “to be.” For security controls, this involves comparing the present state of controls with a desired state of controls. Well-known frameworks help organizations set up a desired state. This process also helps better manage operational risk. This includes adherence to regulatory and industry requirements to protect sensitive systems and information as well as privacy data.

At a minimum, common baseline security controls should be in place. Any gaps to the following types of controls should be clearly documented:

- **Information security policies**—This provides direction for the entire organization regarding goals, risks, and applicable laws and regulations.
- **Information security responsibilities**—This defines how staff will execute the policies, assign responsibilities, and promote accountability.
- **Information security awareness, education, and training**—This defines the program to provide initial and ongoing security education across the organization.
- **Correct processing in applications**—This prevents errors and unauthorized misuse of applications.
- **Vulnerability management**—This reduces the risk of known vulnerabilities being exploited.
- **Business continuity management**—This provides methods to continue critical operations in spite of business interruptions.
- **Security incident management**—This ensures security-related events are

communicated and acted upon to allow corrective action to be taken by security staff.

The report should clearly identify any major gaps. The report should also provide supporting documentation as to the overall implementation of controls, which includes noting any gaps. A simple approach could include, for example, a spreadsheet with a list of controls and columns to identify a control that is in place, partially in place, or not in place. Another common method is to use a percentage. [Table 7-7](#) provides an example of identifying gaps for security incident management controls based on ISO/IEC 27002.

TABLE 7-7 Sample gap analysis of security incident management controls.

CONTROL	COMPLETION STATUS
Report information security events as quickly as possible	100%
Report security weaknesses in systems and services	50%
Establish incident response responsibilities and procedures	100%
Learn from your information security incidents	0%
Collect evidence to support your actions	25%

Compliance Requirement

Proper security controls are essential to maintaining and safeguarding the IT environment, which exists to help drive the organization's goals. You can group compliance broadly into two categories: compliance with internal policies and standards and compliance with regulatory and industry requirements. Controls explicit to compliance should be included as part of a policy to ensure adherence with applicable legislation and internal governance.

At a minimum, organizations should have a program to manage compliance with internal policies and standards. Specifically, this includes identifying areas of noncompliance and methods for correction. Additionally, technical controls should be in place to ensure systems are compliant with standards. This would also include a program for penetration testing and vulnerability assessments. In addition, the organization should have a documented control program in place. This program should manage the audit requirements of information systems.

The final report should identify how the report and associated audit and assessment activities fit into the organization's control. Next, it should include the current state of compliance with legal requirements and compare this with where the organization needs to be.

WARNING

You should get legal counsel during the process of a gap analysis regarding regulatory requirements. Legal requirements vary from state to state and across different countries. Organizations that operate within a single country may still have to meet certain requirements based on the flow of information to other countries.

Has the organization identified all legal, regulatory, and industry-specific requirements? Without these key controls, it will be difficult for the organization to implement and enforce further controls. Additionally, the organization should document the gaps for the following requirements:

- **Respecting intellectual property rights (IPRs)**—**Organizations, regardless** of size, depend on proprietary software and other intangible assets. Examples of intellectual property include those items protected by copyrights, trademarks, patents, and trade secrets. **Intellectual property rights (IPRs)** are the exclusive privilege to intangible assets.
- **Protecting and retaining organizational records**—Laws and regulations set time periods for which organizations must hold and protect specific types of data.
- **Protecting personal information**—Numerous laws have been enacted to protect the collection, processing, and storage of personal information.
- **Preventing users from using systems for unauthorized purposes**—**Because** of legislation that provides protection against computer misuses, organizations are required to meet requirements for security monitoring access notification.
- **Managing the proper use and import or export of cryptographic controls**—Although laws have been relaxed in recent years, there are legal restrictions on the export of cryptographic technology to rogue states or terrorist organizations. In fact, strong cryptography for many years was considered munitions and was part of a list that included items such as firearms, tanks, chemical agents, and nuclear weapons.

Risk, Threat, and Vulnerability Mitigation Requirement

The documented gap analysis should include basic security controls introduced in the beginning of this section. It should also consider controls relevant to the risks of the organization. However, this depends on an organization's ongoing program for establishing security requirements, assessing security risks, and managing controls.

Compliance Assessment Throughout the IT Infrastructure

The results of a compliance assessment should clearly address whether specific requirements are met. For example, consider the following:

- **Compliant**—This indicates that there is enough suitable evidence to show that a particular requirement has been met.
- **Noncompliant**—This indicates that enough suitable evidence was collected to show that a particular requirement has not been met.
- **Not determined**—This indicates that not enough evidence was collected to make an appropriate compliance determination.

TABLE 7-8 A sample documented PCI DSS compliance test result.

PCI DSS REQUIREMENT	TESTING PROCEDURES	STATUS	COMMENTS
Do not use vendor-supplied defaults for system passwords and other security parameters.	Attempted to log on to a sample of selected critical systems using the default vendor-supplied accounts and passwords taken from vendor documentation	Compliant	The point-of-sale systems do not support vendor-supplied default passwords.

- **Not applicable**—This indicates that a requirement doesn't apply. For example, compliance requirements to wireless networks would not apply if the organization doesn't maintain wireless networks. In addition, this would be an appropriate response if a determination could not be made within the scope of the audit. This differs from not having enough evidence in that a particular requirement may be dependent upon an activity or event. Consider the example where certain external organizations must be notified in the event of a breach. Making an appropriate determination would not apply if, for example, the organization has not encountered a breach.

The testing procedures used should be documented. This should also include comments regarding the determination. For example, consider compliance with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS requires that vendor-supplied default passwords be changed before installing a system on the network. The report would include this along with the other requirements followed by the corresponding testing procedures and results. [Table 7-8](#) provides an example of the documented results for this requirement.

Presenting Compliance Recommendations

Audits sometimes reveal major risks or compliance gaps. In those cases, the final reports may include recommendations supported by the audit findings. The recommended actions should be logically tied to a finding for which the problem has also been identified. A recommendation is more valuable to the organization when it is specific, sensible, and cost effective. Ultimately, the objective is to consider the processes and inputs up to this point and clearly communicate the following:

- Recommended actions to lessen control weaknesses
- Recommended actions to comply with applicable laws and regulations
- Comparisons and gaps to standards and accepted frameworks and recommendations to narrow the gap

Recommendations should be actionable. They should not include statements such as “controls should be strengthened.” Tactical recommendations are important and needed. However, the report should also provide strategic recommendations. Specifically, these consider the broader picture of the organization objectives and how identified gaps or vulnerabilities affect the organization’s ability to achieve those goals.

Management action plans and appropriate follow-up are critical to close the process. Recommendations provide the action that management should take to deal with deficiencies. It is the documented action plan, however, that provides the guidance for correcting those deficiencies. This includes assigning responsibility for each recommendation and assigning deadlines. Agreed-upon actions should be documented within the recommendations if this information is provided by management prior to the final report.

As part of the document-gathering process of an audit, the auditor should consider previous audit results and past recommendations. Likewise, documented results and recommendations will be examined with the next audit. This provides a process for continual awareness to changing environments and constant improvement.



CHAPTER SUMMARY

After the auditing team has completed the audit, an audit report will be issued to the organization. Depending on the scope and objectives of the audit, this report can take on many different forms. Regardless, effective communication of the results is vital to prevent any misunderstanding. Proper communication of the results will also ensure adequate follow-up actions.



KEY CONCEPTS AND TERMS

Executive summary

Finding

Intellectual property rights (IPRs)

Process Capability Model



CHAPTER 7 ASSESSMENT

1. Which of the following is *not* a purpose of the audit report?
 - A. Provide an action plan for auditors to implement controls.
 - B. Communicate the results.
 - C. Prevent misunderstanding of the results.
 - D. Facilitate follow-up corrective action.
2. An abstract of an audit report provides a brief review intended for senior-level management who might not have the time to read and understand the entire report.
 - A. True
 - B. False
3. An executive summary should never be more than one page long.
 - A. True
 - B. False
4. Which of the following best describes an audit finding?
 - A. The procedures used to find IT controls
 - B. A documented conclusion that identifies deficiencies
 - C. A verbal recommendation to improve controls
 - D. The auditor's fee
5. Which level using the COBIT Process Capability Model would be assigned to a business that does not recognize the need for IT security, nor has a recognizable system security administration process?
 - A. Level 0
 - B. Level 1
 - C. Level 2
 - D. Level 3
6. Which one of the following is the product of the likelihood of a threat occurring and the impact the threat could have?
 - A. Occurrence
 - B. Risk
 - C. Vulnerability

- D. Likelihood of impact
- 7.** Which one of the following is *not* a privacy principle as identified by GAAP?
- A. Secrecy
 - B. Choice and consent
 - C. Collection
 - D. Use and retention
 - E. Disclosure to third parties
- 8.** Which of the following best describes a business that is found to have unlicensed software installed throughout the environment?
- A. They have violated export restrictions on cryptographic software.
 - B. They are not adequately protecting personal information.
 - C. They have violated intellectual property rights.
 - D. Answers B and C
- 9.** Which of the following best describes when compliance of a control cannot be determined due to a lack of collected evidence?
- A. Not determined
 - B. Not applicable
 - C. Compliant
 - D. Answers A and B
- 10.** The final audit report includes recommended actions, which should be associated with which of the following?
- A. Findings
 - B. Vulnerabilities
 - C. Threats
 - D. None of the above

CHAPTER 8

Compliance Within the User Domain

E

NSURING COMPLIANCE IS MORE THAN just checking items off a list. It is a dynamic process of making sure the items in each domain meet or exceed your goals. Because conditions can change in any organization, how well you are meeting your goals can change as well. You should make all decisions related to security controls to satisfy your security policy and any other relevant compliance requirements. Ensuring compliance with your security policy keeps security-related actions headed in the right direction.

Within the seven domains of a typical information technology (IT) infrastructure, the User Domain defines the components that directly interact with information system users. User Domain components both govern and are influenced by user behavior. The best User Domain controls direct and restrict user actions and result in compliant behavior. In short, your goal in the User Domain is to persuade users to act in a way that meets or exceeds your standards of behavior. In this chapter, you'll learn about different opportunities to affect user behavior and how that behavior affects your organization's security.

Chapter 8 Topics

This chapter covers the following topics and concepts:

- How compliance law requirements relate to business drivers
- Which items are commonly found in the User Domain
- What separation of duties means
- What least privilege is
- What need to know is
- What confidentiality agreements are
- What employee background checks are
- How acknowledgment of responsibilities and accountabilities relate to compliance
- How security awareness and training for new employees relate to compliance
- What information systems security accountability is
- How to ensure adherence to documented IT security policies, standards, procedures, and guidelines
- What best practices for User Domain compliance are

Chapter 8 Goals

When you complete this chapter, you will be able to:

- Identify compliance law requirements and business drivers

- Compare how items found in the User Domain contribute to compliance
- Describe methods of ensuring compliance in the User Domain
- Summarize best practices for User Domain compliance

Compliance Law Requirements and Business Drivers

Information systems provide information to users. Without users, there would be no reason to invest in collecting, manipulating, and storing data. Information passes from the outside world to the information system through user actions. Keyboards, mice, and scanners are just a few of the common methods users employ to get information into the various systems. A secure system needs controls that limit the type of information users can provide and retrieve.

The User Domain is the domain in the IT infrastructure that formalizes how information flows in and out of computer systems. This domain defines components you need to control to ensure your environment is compliant with applicable requirements. [Figure 8-1](#) shows the User Domain in the context of the seven domains in the IT infrastructure.

User Domain controls designed to help ensure compliance place limits on acceptable user actions. A User Domain control is any mechanism that interacts with a user and reacts when a user's actions meet certain conditions. The overall purpose of User Domain controls is to restrict user behavior to approved, or compliant, behavior. The control's reaction depends on what type of control it is. Controls generally fall into the following functional types:

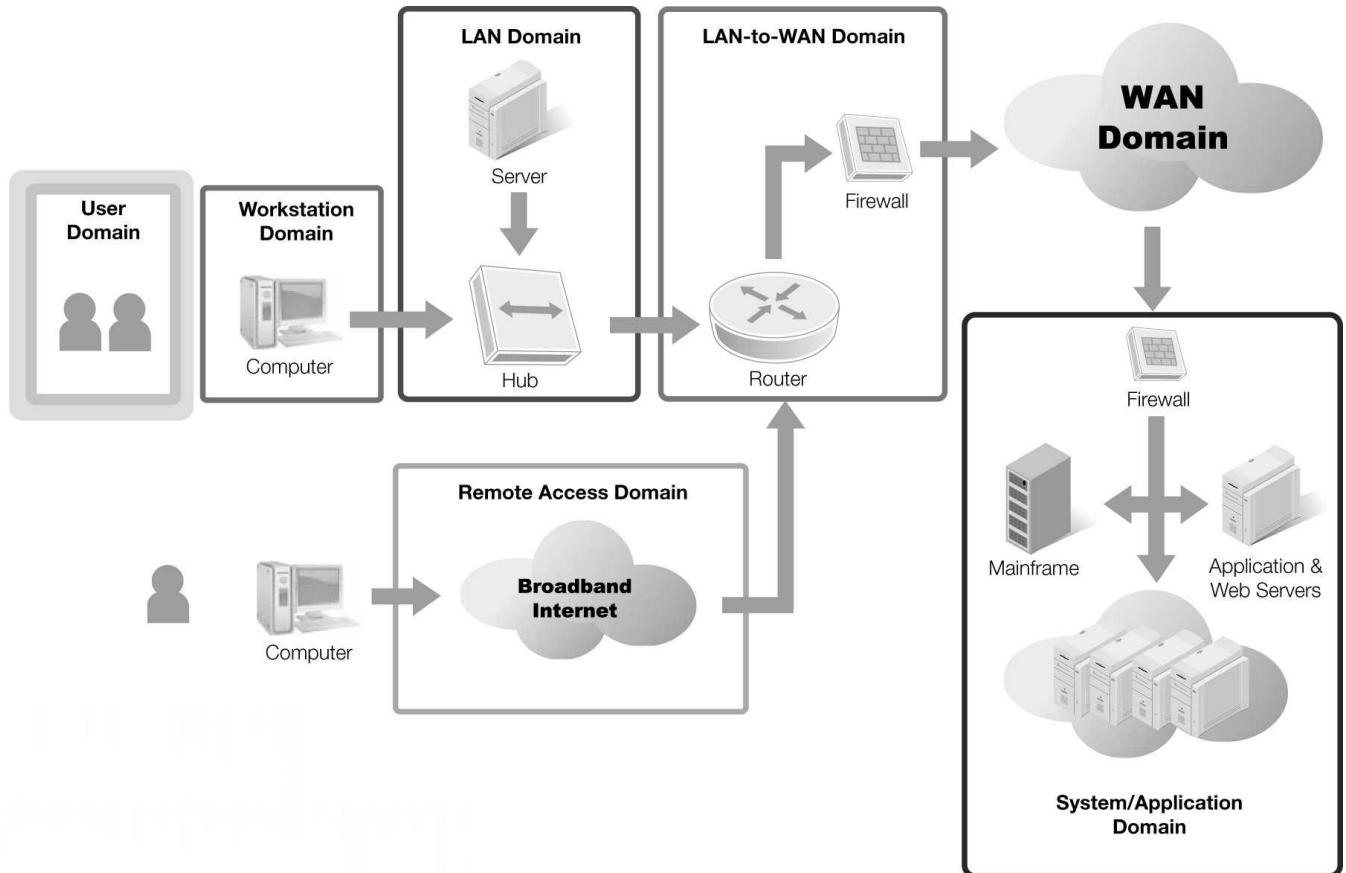


FIGURE 8-1 The User Domain within the seven domains of a typical IT infrastructure.

- **Preventive controls**—Mechanisms called **preventive controls**, such as locked doors or computer access controls, keep an undesired action from happening.
- **Detective controls**—Mechanisms called **detective controls**, such as motion detectors or usage log analysis tools, recognize when an undesired action has occurred.
- **Corrective controls**—Mechanisms called **corrective controls**, such as the procedure to remove viruses or a firewall to block an attacking system, repair damage caused by an undesired action and limit further damage.

Figure 8-2 gives an overview of preventive, detective, and corrective controls.

By limiting what users can do, compliance-related security controls restrict users to appropriate actions. These restrictions can include limits on what users can access and what actions they can perform. Although limiting users to meet compliance requirements might be desirable or even necessary, it can make it more difficult to complete required business functions. One of the difficulties of ensuring security in the User Domain is designing secure controls that still allow and promote necessary business functions.

Preventive Controls

- Stop actions

Detective Controls

- Recognize actions

Corrective Controls

- Fix the result of actions

FIGURE 8-2 Types of security controls.

It is important that you implement compliance requirements in a way that minimizes the impact on **business drivers**. Business drivers are the components, including people,

information, and conditions, that support business objectives. Any negative impact on business drivers can also have a negative impact on your organization's ability to satisfy business objectives. Carefully research the impact on business drivers before you implement any compliance controls.

Compliance requirements dictate how your organization conducts its activities. Whether the compliance requirement comes from legislation, regulation, industry requirements, or even your organization's standards, the end result is the focus. In most cases, your organization can control activities to ensure compliance in multiple ways. Always consider alternative controls to achieve the end result that compliance requires. You'll likely find that some controls are less costly and less intrusive than others. Don't just accept the first control that does the job. Often, other controls are just as good but intrude less on your organization's activities.

You can meet many compliance requirements using one of several controls. If one control has a negative impact on business drivers, consider another control. You can often justify eliminating one control if another control will achieve the same goal.

For example, Payment Card Industry Data Security Standard (PCI DSS) requires that you store credit card information as encrypted data. Implementing data-level encryption in a legacy application can be expensive and require a substantial effort. If you run Windows Server, one possible alternative is to use Microsoft BitLocker Drive Encryption. BitLocker could be a compensating control for application-level encryption. [Figure 8-3](#) shows a comparison of controls using PCI DSS as an example.

PCI DSS Requirement—Encrypt Stored Data

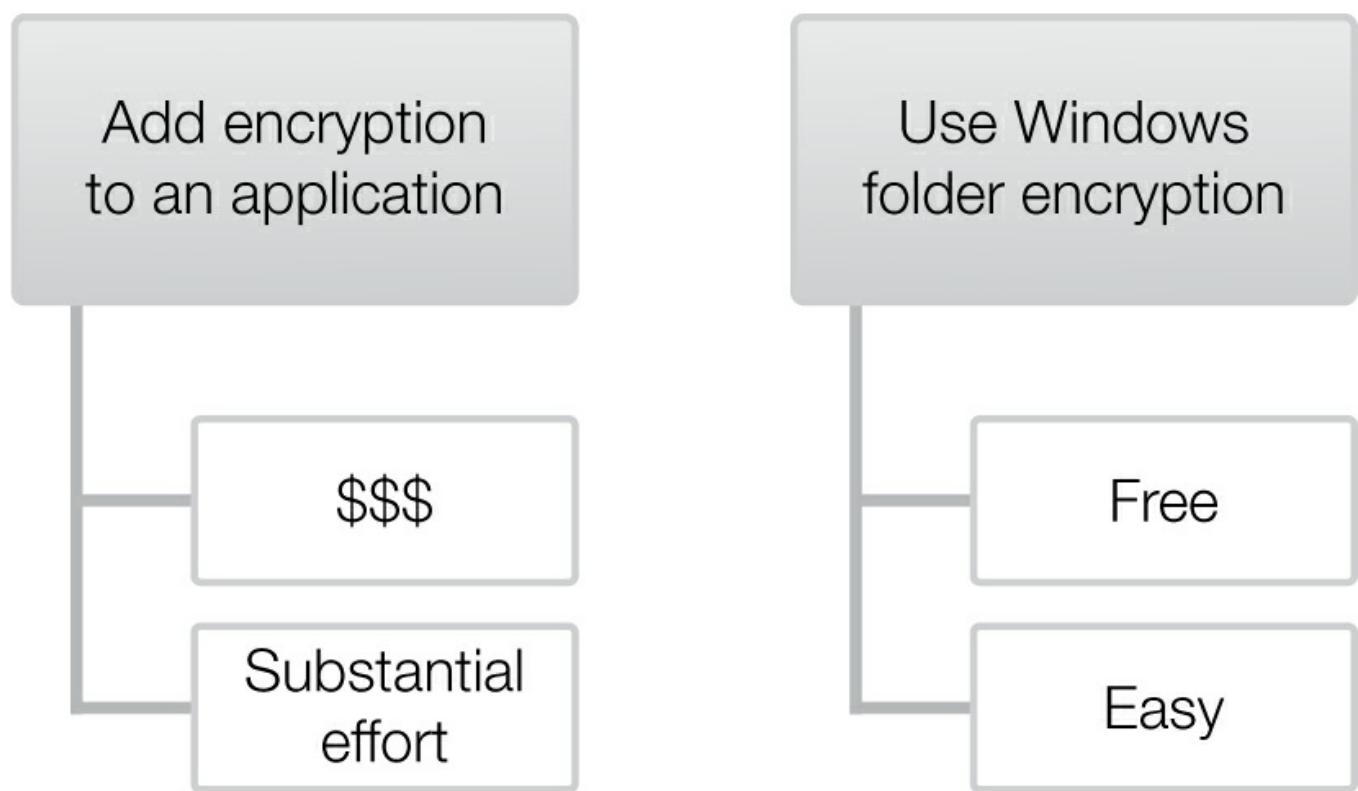


FIGURE 8-3 Alternative controls.

Many User Domain compliance requirements relate to information access and privacy. The controls you implement will likely restrict what data and programs your users can access. Controls can also provide information on actions users have carried out. User Domain compliance focuses on accountability. Compliant systems monitor and control actions that relate to compliance.

Monitoring actions as they occur allows preventive controls to evaluate action requests and deny unsuitable actions. Operating system access controls fall into this category. The operating system denies a request to open a file if the user does not have sufficient permissions to open the file. The system can monitor access to many other objects as well. If the system uses a log file to track every access attempt, you can analyze the data. Logging object access is a type of detective control.

Implementing Proper Security Controls for the User Domain

It takes careful planning in any domain to develop multiple layers of proper security controls. Control layers should complement other layers and work together to avoid exposing a single point of failure. In the User Domain, an **acceptable use policy (AUP)** for each type of user serves as a training guide and direction document for other controls. Simply put, the AUP is a statement of which actions are acceptable and which ones are not.

The AUP is not the only security control for the User Domain but it is an important one. Solid User Domain controls help ensure compliance with your organization's security policy. As you design controls, make sure you develop multiple layers to protect each resource. Your goal should be to force an attacker to defeat several controls to compromise a resource. That way, no single control failure exposes a resource to an attack. But before you can design solid controls, you need to explore components commonly found in the User Domain.

Items Commonly Found in the User Domain

The User Domain contains several common items or components. You should consider each component when evaluating activities for compliance. People and documentation are the most common items in the User Domain. Each of these two broad categories includes several smaller types of items with unique characteristics. The following are different types of people in the User Domain:

- **Employees**—This group has the greatest stake in the organization. Most long-term employees feel a greater sense of responsibility toward their employer than shorter-term personnel do. Employees generally have more privileges and access to organization resources. Although you can trust most employees, an unethical employee can cause substantial damage because of access to information and knowledge of the organization.
- **Contractors**—Contractors may bring specialized skills to an organization but they also pose potential risks. Because contractors may have access to sensitive information, you must monitor them and give them only enough access to do their jobs. Contractors may be less loyal to the organization than employees due to contractors' limited employment. All these reasons present contractors as a greater risk for security violations.
- **Guests/third parties**—Other parties might have no duties related to sensitive information but might still have access to an organization's network. Many organizations commonly provide Internet access to visitors. You should use strict

controls to ensure guests do not have access to any sensitive information.

Figure 8-4 illustrates items commonly found in the User Domain.

The User Domain contains more than just people. It is important that people who are resources for an organization have formal directions for how they carry out activities. These activities should support the meeting of business goals. You need a collection of documents that outlines activities that support business activities to determine whether an action is acceptable or unacceptable. The User Domain also needs documented policies to direct the actions of people. The following are different types of documentation in the User Domain that affect compliance:

- **Human resources (HR) manuals**—HR acquires and manages an organization's personnel. Personnel management includes security awareness and education. Because many security incidents involve users, it is important to provide written documentation of an organization's policies and procedures. HR manuals provide information on how people within an organization should conduct themselves in any situation.
- **IT asset AUPs**—AUPs provide guidance for personnel on proper use of resources. They also define what constitutes improper use. An IT asset AUP covers the use of all IT assets, such as computers, wireless access points, networks, and printers.

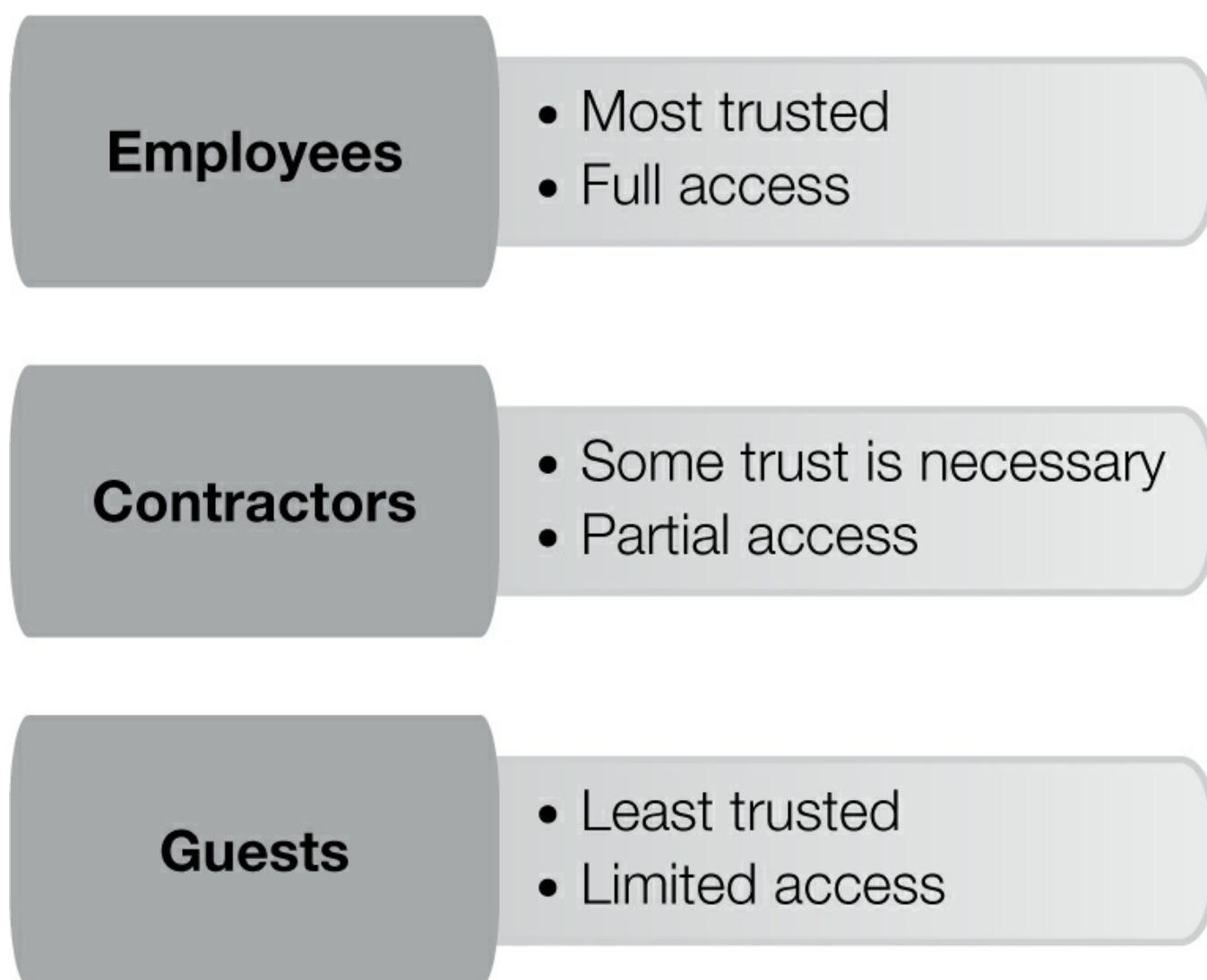


FIGURE 8-4 Common items in the User Domain.

- **Internet AUPs**—Internet AUPs define proper and improper use of an organization’s Internet access.
- **E-mail AUPs**—E-mail AUPs define proper and improper use of an organization’s e-mail capability.

A solid basis for compliant activity requires a well-organized User Domain with clear roles and expectations. In the following sections, you’ll learn about important concepts to build a secure environment of compliant behavior.

Separation of Duties

A common theme in compliance requirements is to reduce the ability of any one element to compromise data security. In the User Domain, this means that no single person should have the ability to bypass security controls that protect data. Each computer user’s role should limit the scope of permitted actions.

Most computer systems restrict access to deny unauthorized users. The first step in gaining access to data is to identify yourself to the information system and authenticate your identity. This process commonly involves providing a user ID and a password. Once you are identified and authenticated, the operating system grants authority in the form of permissions and rights. These permissions and rights are defined by your assigned roles. You can only accomplish what your assigned roles allow.

The concept of **separation of duties** requires that users from at least two distinct roles be required to accomplish any business-critical task. This means that users from at least two roles must collude to compromise data security. Although collusion is still possible, it is far less likely than if a single user could gain exclusive access to sensitive data without anyone else looking. Going further, separation of duties helps avoid conflicts of interest. For example, the role in charge of administering a system should not be the same role that audits that system for potential compliance violations. [Table 8-1](#) contains some examples of separation of duties in IT environments. [Figure 8-5](#) illustrates separation of duties in an IT environment.

technical TIP

You can define User Domain roles at the operating system level to limit what users can and cannot do. One method of access control uses operating system groups to define access permissions for objects, such as files, folders, and printers.

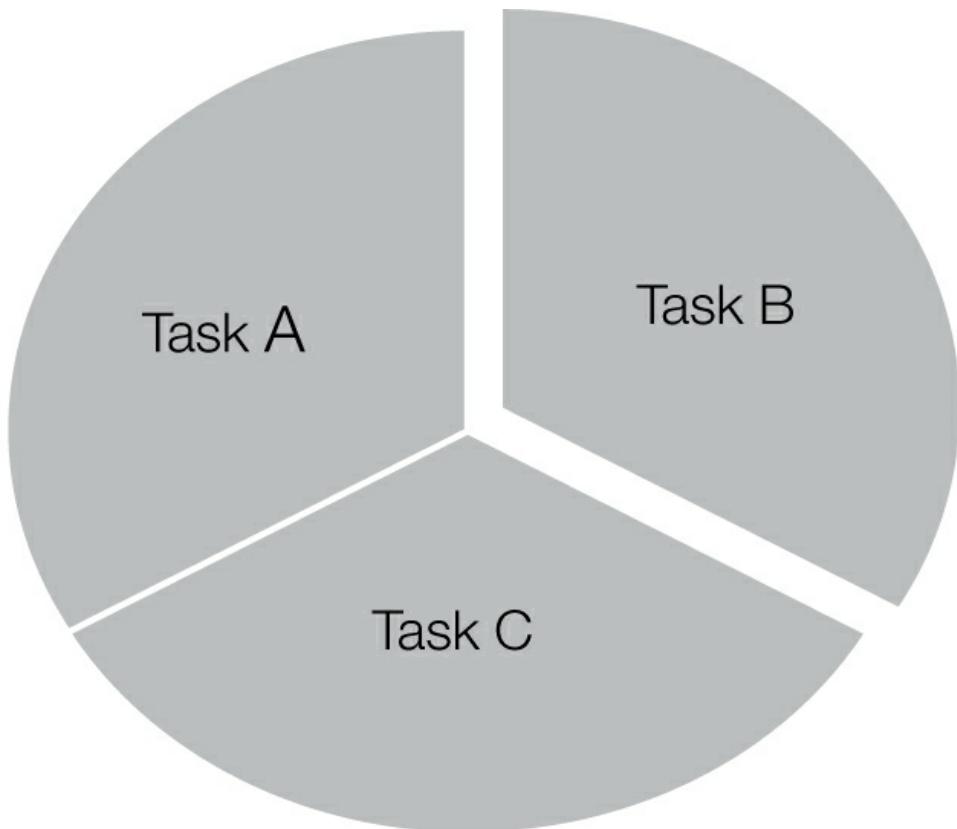
Separation of Duties During the Cold War

You can find a common example of separation of duties in many movies. During the Cold War between the United States and the Soviet Union, the militaries on both sides operated silos that housed nuclear-tipped missiles. Because each missile could deliver multiple devastating warheads, it was imperative to avoid an accidental launch at all costs.

Once a launch command made its way up the chain of command, the final action to launch the missiles required two people to insert and turn a unique key at the same time. Both keys were required for launch, and the keys were too far apart for one person to insert and turn them at the same time. This design reduced the possibility that a single person could initiate a launch because only one key wasn’t sufficient to launch the missiles.

TABLE 8-1 Examples of separation of duties in an IT environment.

ROLE RESTRICTION	DESCRIPTION
Only grant limited access for external personnel to the computer and files they need for the current project.	External personnel can help complete projects but should have limited access to resources. This restriction helps reduce the number of people who have access to each part of a system and reduces the opportunities for data compromise.
Prohibit all access to production environments for developers.	Developers have the ability to write programs that access sensitive data and should not have the ability to bypass configuration-management controls. Configuration-management controls require a separate role to promote software from development to production.
Do not allow general administrative users to create backups of critical data.	It is easy to create backups on media that fit in a pocket. Create a role for backup operators and only allow a small number of individuals to create backups.



- Separate critical business processes into units of work
- A different person performs each unit of work

FIGURE 8-5 Separation of duties.

Least Privilege

The first step in implementing separation of duties is to remove unnecessary user privileges. Any unnecessary privilege provides an opportunity for a user to violate the AUP and perform unauthorized data access. It makes sense to use access controls to prevent unauthorized

data access. The process of allowing only the level of access your users require might be tedious, but it is necessary to secure sensitive data.

 **TIP**

When you define permissions based on roles, or groups, you allow object owners and administrators to grant access rights at their discretion. This type of access control is a **discretionary access control (DAC)** and is common in commercial environments.

The ultimate goal is to define access control where each user has the permissions to carry out assigned tasks and nothing else. This is the principle of least privilege. User permissions beyond what is required to carry out necessary tasks are excessive and potentially unsecure.

Putting least privilege into practice can be challenging. Organizations with many users often use roles, or groups, to define access permissions. Administrators define roles that represent small tasks, such as “accounts receivable user” and “accounts receivable manager,” and grant specific permissions to each role. Individual user accounts can belong to one or more roles and inherit the permissions from each of the role definitions.

Government organizations and some commercial organizations implement the principle of least privilege in a different way. They use a system not based on roles, but on data classification and user clearance. The operating system makes the decision to grant or deny access to any data object by matching the object’s classification to the user’s clearance. Because this method of access control is based on object and subject attributes and not on anyone’s discretion, this is a **mandatory access control (MAC)**. [Table 8-2](#) shows the classification system the U.S. government uses for MAC.

TABLE 8-2 U.S. government **MAC** clearance and classification levels.

CLASSIFICATION	DESCRIPTION
Unclassified	No security label is needed. This object is accessible by anyone.
For Official Use Only	This is for objects that should not be accessible by anyone outside an organization.
Confidential	This is for objects that contain information that could cause harm to an organization or nation if divulged.
Secret	This is for objects that contain information that could cause serious harm to an organization or nation if divulged.
Top Secret	This is for objects that contain information that would likely cause extreme harm to an organization or nation if divulged.

Nongovernmental organizations that need to protect information at different sensitivity levels can also use MAC to secure information. The ISO 27002 standard contains suggestions for five basic classifications. These classification levels are just suggestions for organizations that do not already have a classification strategy in place. [Table 8-3](#) shows the ISO 27002 suggested classification levels.

TABLE 8-3 ISO 27002 suggested **clearance and classification levels**.

CLASSIFICATION	DESCRIPTION
Public Documents	This is for objects in the public domain.

Internal Use Only	This is for objects that have not been approved for release to the public.
Proprietary	This is for objects that contain information that might be harmful to an organization if divulged to the general public.
Highly Confidential	This is for objects that contain sensitive information that is critical to an organization. Divulging such information could have a significantly negative impact on an organization.
Top Secret	This is for objects that contain extremely sensitive information that would cause extreme damage to an organization if divulged.

FYI

Need to know limits access to secure objects and limits damage in the case of a breach. Assume the project manager used in this section's example leaves the organization. If she chooses to violate ethics and disclosure regulations, she could disclose the contents of all objects to which she had access. The principles of need to know and least privilege protect the organization by limiting how much information a single individual can compromise.

Need to Know

Whereas DAC supports the detailed control necessary for least privilege, simple data classification and user clearances do not. You need an additional control to ensure users possess only the privileges they need to do their jobs. For example, a project manager needs access to documents related to the current project only. If the documents for several unrelated projects are all labeled as "highly confidential" and the project manager holds a "highly confidential" clearance, all project documents would be available.

Although this situation might seem reasonable, it does allow project managers to access documents that are unrelated to their current projects. This capability violates the principle of least privilege. Most systems that use DAC also use the concept of **need to know**. In addition to possessing a clearance level that matches or exceeds the classification label of an object, a subject must have the need to know for the object as well. Simply put, need to know means that you have a need to access an object to do your job. Adding the concept of need to know to DAC does provide full support for the principle of least privilege.

Confidentiality Agreements

Employees who work with sensitive information can be both a great asset and a great risk. A person who understands the inner workings of your organization can protect sensitive information or defeat your security controls. Someone who knows your organization could make violations difficult to detect. Contractors who have access to sensitive information can be just as dangerous. How should your organization protect sensitive information from insiders? The answer is to implement a defense-in-depth strategy. Solid access controls and the principle of least privilege are both important, but neither is enough.

Some information leaks occur because of simple ignorance or carelessness. If workers don't know that information is sensitive, they might treat it with less care. When hiring personnel, you should communicate your organization's security policy clearly. The employee or contractor **confidentiality agreement** is a document that accomplishes this.

Another name for this document is a **non-disclosure agreement (NDA)**.

A confidentiality agreement is a legally binding document. By signing this document, each party agrees to keep certain types of information confidential. A confidentiality agreement is a necessary part of any relationship that involves sensitive information.

Confidentiality agreements allow organizations to disclose sensitive information to a small number of parties without concern that an information leak might cause harm. For example, these agreements allow organizations to share specifications of unreleased products to business partners. Sharing this type of information allows business partners to develop companion products before the release of original products. Most major software vendors, such as Microsoft and Apple, do this to allow their development partners to write software for new operating systems before the release date. The confidentiality agreement protects the operating system vendor by prohibiting partners from releasing information about the new product.

NOTE

Two types of professional relationships involving sensitive information don't require a confidentiality agreement. Privacy laws cover relationships between clients and attorneys and between patients and doctors. These relationships do not need other agreements to keep information confidential.

Another important feature of a confidentiality agreement is that it can protect patent rights. Publicly disclosing an invention can result in forfeiting any patent rights. An organization must keep information about the invention confidential until filing a patent application. Confidentiality agreements with anyone who has access to confidential information can protect your organization from a damaging public disclosure.

A confidentiality agreement defines the types of information parties can and cannot disclose. A confidentiality agreement also specifies how parties may use confidential information. The agreement defines expected behavior and the consequences of violating the agreement. A well-written confidentiality agreement lowers the risk of disclosing confidential information.

WARNING

Binding confidentiality agreements should define time frames for the agreement. Confidentiality agreements are not valid forever. A good agreement specifies a date range within which parties must make disclosures and a date range within which disclosure restrictions are in force. A lack of either time frame could invalidate the agreement.

Employee Background Checks

Many organizations perform a **background check** on prospective employees before hiring them. The purpose of a background check is to uncover any evidence of past behavior that might indicate a prospect is a security risk. In reality, all personnel are security risks because they must be trusted with sensitive information. A background check can uncover information that indicates a person might be an undue security risk.

Background checks can vary in depth. For example, a background check might simply

verify a Social Security number as authentic and belonging to the applicant. Or, a background check might involve conducting a police criminal check and reviewing a prospective employee's complete history. Each organization sets the scope of background checks. The job description and the organization's desire to use a prospect's history to predict future actions affect the scope of the investigation. You can conduct background checks using internal resources or by engaging external specialists. External resources can reduce your ongoing expense and may provide higher-quality information due to the use of specialists. However, external resources who conduct background checks operate under additional restrictions.

The **Fair Credit Reporting Act (FCRA)**, which defines national standards for all consumer reports, also governs how you conduct background checks. FCRA governs background checks because they are labeled as consumer reports, even though a background check may consist of more than credit history information. FCRA sets time limits on negative information that investigators can include in their report. Although some states may lengthen FCRA time limits, investigators cannot include the following:

- Bankruptcies that are more than 10 years old
- Civil suits or judgments that are more than 7 years old
- Paid tax liens or other negative financial information that is more than 7 years old

Background checks often include much more than just financial information. Most employers are more interested than ever in a prospective employee's general past and current behavior. In many cases, social networking sites, such as Facebook or Twitter, can provide information on a prospect's behavior. Fair or not, more and more employers are looking into past behavior to attempt to decide how trustworthy a prospect may be.

Although background checks are important and might provide interesting insight into a person's background, you must perform them with care. FCRA requires that you obtain permission from the subject of a background check before you begin the investigation. In addition, if you decide not to extend an offer due to information contained in the background check report, you must provide the reason and the contact information for the investigating organization. You must also give the prospect the opportunity to dispute any negative information in the report. This safeguard helps prevent incorrect information from harming an unsuspecting individual.

Background checks can reveal quite a lot about a prospective employee. A prospect with prior criminal history might not be a good candidate for a role that allows access to very sensitive information. Knowing the background of prospective employees is an important step in granting authorization to sensitive information. Although a background check won't catch every potential attacker, it can help identify some of the most likely high-risk candidates.

Acknowledgment of Responsibilities and Accountabilities

Auditing is the process of examining systems to verify they are in compliance with defined policies. In short, auditing ensures that activities comply with policy. This process provides value only when it objectively reviews evidence of actions. An auditor who overlooks any evidence of noncompliance isn't very effective. Because of the potential of negative findings, it is important that all parties engaged in auditing activities understand their responsibilities to the audit process.

Don't view auditing simply as a search for problems. Auditing is an opportunity to identify

noncompliance issues before they escalate and possibly cause damage. This positive attitude toward auditing must start with upper management, who should share it with all affected parties. If upper management does not fully support the efforts of auditors, it is unlikely anyone else will.

Upper management can influence the quality of the audit process by assigning responsibilities and accountabilities. Every employee bears some responsibility in the IT security audit process. Every agent of your organization must maintain the security of your information. Because the IT security auditing process verifies compliance with security policies, all employees bear responsibility for carrying out your policies.

▶ NOTE

Repetitive auditing and taking action on the results of audits are proactive forms of continuous improvement. The general idea is that constantly adhering to policies results in higher-quality output—not just fewer violations.

Each task in the audit process has one or more people who are responsible or accountable for that task. Many organizations use a **RACI matrix** to document tasks and personnel responsible for the assignments. RACI stands for responsible, accountable, consulted, and informed. To create a RACI matrix, do the following:

1. List tasks along one axis and personnel or roles along the other axis.
2. Assign a level or responsibility for each role and task.
3. Assign each person or role a level of responsibility and accountability for each task.

The entries in the matrix will contain one of the following:

- **R (Responsible)**—This is the person who actually performs the work to accomplish the task. It may be multiple people.
- **A (Accountable)**—This is the person who is accountable for the proper completion of the task. Only one person is accountable for each task. The Accountable is likely the Responsible's manager.
- **C (Consulted)**—This is the person who provides input that is helpful in completing a task. It may be multiple people.
- **I (Informed)**—This is the person who desires to be kept up to date on a task's progress. This may be multiple people.

Table 8-4 shows a simple RACI matrix for an IT audit.

The RACI matrix clarifies the responsibilities and accountabilities for a set of tasks. A RACI matrix provides upper management with a tool that communicates and conveys tasks. Without the acceptance of audit responsibilities and accountabilities, the auditing process might encounter resistance. Management and other employees might view the audit process as punitive.

TABLE 8-4 Simple RACI matrix for an IT audit.

Task/Role	Management	Project Manager	Auditor	User
Develop audit plan	A	R	C	I
Develop audit activities schedule	A	R	C	I
Conduct audit activities		A	R	C
Review audit results	A/R	R	R	C
Identify noncompliant elements	A	I	R	C
Develop plan to address noncompliant elements	A	R	C	I
Develop noncompliant mitigation activities schedule	A	R	C	C
Conduct noncompliant mitigation activities		A	R	R

Security Awareness and Training for New Employees

Employees often have the greatest access to an organization's critical resources. Your organization places substantial trust in its employees and takes on substantial risk in doing so. Many security incidents originate from internal personnel, including employees. Not all incidents are malicious attacks. Some are simply a failure to comply with the organization's stated security policy.

It is important to educate new employees on your organization's security policies and procedures. It is difficult for employees to comply with a policy if they are unaware of what the policy contains. Training employees on security matters can help avoid many security policy violations, including the following:

- Weak passwords
- Inappropriate use of the Internet
- Inappropriate use of e-mail
- Divulging confidential information

The HR department usually follows an established procedure when handling new employees. Security awareness and security procedures training should be a part of this process. You should provide training for each employee on security topics, including the following:

- The organization's commitment to information security
- The justification for security-related activities
- Important security procedures

FYI

Security awareness and procedures training are not only for new employees. As technology and threats change, security procedures must address those changes. Employers should provide security training for all employees to maintain a security-conscious work force. Don't wait for an annual opportunity to train

existing employees on security awareness topics. Schedule recurrent training for topics you should refresh periodically. You can use ongoing techniques, such as banners and reminders, to continually keep all employees aware of how important security really is.

Security training should include justification. It is important that employees understand the value of security to the health of your organization. Employees should acknowledge they have received security training and agree to abide by your security policy and procedures. Many organizations make use of the employees' acknowledgment to uphold the security policy, requiring it as a condition of employment. Because the security of sensitive resources is important to your organization, it should be important to your employees.

Information Systems Security Accountability

Security-related activities often have lower importance than activities that directly make money. Unless upper management clearly states the importance of security, security personnel might find it difficult to obtain funding and support to maintain secure systems. Most important, an organization's upper management is responsible for protecting the security of the organization's resources. Management is beholden to the stockholders, regulatory agencies, government entities, and the public.

In addition, management should assign accountability for each security-related activity. Creating and maintaining a secure environment requires acceptance of accountability.

Requiring That Human Resources Take a Lead Role

HR is responsible for acquiring and managing all of your organization's personnel. This includes initial and recurrent training. Because HR is responsible for proper employee and other personnel training, the department should be accountable for ensuring each person receives training.

In fact, HR takes a lead role in the accountability of all personnel actions. Having HR take a lead role centralizes training delivery and employee-related compliance activities. HR also operates above functional management and protects the organization from role favoritism. HR ensures that the organization holds all personnel to the same set of standards.

Defining Accurate IT and IT Security Employee Job Descriptions

HR is also responsible for defining the activities of all personnel, including IT personnel. Accurate job descriptions are necessary to acquire the best employees for each position. Job descriptions also set proper expectations for all personnel. Accurate and up-to-date job descriptions allow HR to develop the most appropriate role-based training and to ensure all employees receive proper training to carry out their tasks.

Job descriptions also set and maintain the expectations and performance standards for each employee. These expectations provide a standard for employee performance measurement. Although specific performance numbers might be outside the scope of a job description, it does contain a framework of expected performance.

Incorporating Accountability into Annual Employee Performance Reviews

In addition to defining the job description, your organization should set performance criteria for evaluating employees. Each employee should have a set of performance criteria that compares performance to goals. These criteria can be valuable during annual performance

reviews.

Performance accountability is important to motivate employees. A motivated employee tends to be happier and more productive. Performing simple tasks with no accountability can lead to boredom and even sloppy work. Your organization should encourage employee accountability and reward staff for taking on more responsibility and being more accountable.

Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines

User behavior is the focus of auditing for IT compliance in the User Domain. In the simplest sense, this consists of examining user actions and comparing those actions with security policies, standards, procedures, and guidelines. If you find any differences with organizational requirements, you should report the differences and analyze their impact.

It is important to train all internal and external users on acceptable behavior. Training should cover the contents of your organization's security statement documents and provide users with the knowledge to comply with the documents. Training that does not cover security expectations is insufficient. Users who hold a privileged role, such as system administrator, should receive additional, specialized training pertinent to their role.



WARNING

It is difficult for untrained users to comply with your security policies. For example, as basic as it might seem, you shouldn't expect users to create and use strong passwords unless you tell them they are required to do so and train them on how to do it.

Good security training should stress the importance of compliance and cover the important parts of these types of security documents:

- **Security policy**—This is a high-level statement that defines an organization's commitment to security and the definition of a secure system, such as the importance of changing passwords periodically.
- **Security standard**—This is a collection of requirements the users must meet, typically within a specific system or environment, such as changing a Windows password every six months.
- **Security procedure**—This refers to individual tasks users must complete to comply with one or more security standards, such as the steps to change a password.
- **Security guideline**—This is a collection of best practices or suggestions that help users comply with procedures and standards, such as suggestions on how to create strong passwords.



NOTE

Some security violations are obvious. However, User Domain auditing reveals many less-obvious noncompliant user actions.

Your access control policies should grant access to information systems depending on users upholding the organization's security policies, standards, procedures, and guidelines. Violation of any of these security elements should carry consequences ranging from a training refresher course to losing access.

Best Practices for User Domain Compliance

Identifying and influencing user behaviors that affect security are important to ensuring compliance within the User Domain. Behaviors that support or violate compliance with your security goals get the most attention. The following best practices do not guarantee compliance with all goals. However, they will lay the foundation to develop and maintain a secure environment:

- Document all laws, regulations, and standards that require User Domain compliance for your organization.
- Define AUPs for each type of IT service or equipment.
- Conduct background checks for all employees and critical contractors prior to engagement.
- Develop security awareness and procedures training for employees and contractors.
- Require security awareness and procedures training and assessment prior to engagement.
- Require users to sign confidentiality agreements before receiving access to any sensitive information.
- Establish unique logon credentials for each user and require strong passwords.
- Grant only the minimum privileges to each user required to accomplish that user's tasks.
- Require action by at least two separate users to complete any business-critical function involving sensitive information.
- Periodically audit user access privileges for compliance to stated goals.



CHAPTER SUMMARY

The User Domain defines information system users and the actions they carry out. A critical factor of maintaining secure systems is ensuring users' compliance with security goals. Because user actions result in accessing information, it is necessary to control and monitor user actions to maintain secure systems. Systems must uniquely identify users and allow access only to information for which they are authorized. Auditing activities should examine all access decisions and the rules that govern such decisions for compliance. Defining limits within the User Domain and validating user activities provide an important security layer in a defense-in-depth approach to system security.



KEY CONCEPTS AND TERMS

Acceptable use policy (AUP)

Background check
Business drivers
Confidentiality agreement
Corrective controls
Detective controls
Discretionary access control (DAC)
Fair Credit Reporting Act (FCRA)
Mandatory access control (MAC)
Need to know
Non-disclosure agreement (NDA)
Preventive controls
RACI matrix
Separation of duties



CHAPTER 8 ASSESSMENT

1. Which type of control only reports that a violation has occurred??
 - A. Preventive
 - B. Detective
 - C. Corrective
 - D. Restorative
2. The term _____ defines the components, including people, information, and conditions, that support business objectives.
3. Which of the following types of policies defines prohibited actions?
 - A. Access control policy
 - B. Password usage policy
 - C. Acceptable use policy
 - D. Violation action policy
4. Which of the following terms ensures at least two people must perform a series of actions to complete a task?
 - A. Separation of duties
 - B. Least privilege
 - C. Need to know
 - D. User clearance
5. When using DAC, a subject must possess sufficient clearance as well as _____ to access an object.
6. Which of the following terms defines a strategy in which you grant access that allows a user to complete assigned tasks and nothing else?
 - A. Separation of duties
 - B. Least privilege
 - C. Need to know
 - D. User clearance
7. Which type of agreement can protect the ability to file a patent application?
 - A. Relinquish ownership agreement
 - B. Security clearance waiver
 - C. Background check agreement
 - D. Confidentiality agreement

- 8.** What condition must exist for a background check to be governed by FCRA?
- A. The investigation includes credit history.
 - B. The investigation is performed by a third party.
 - C. The investigation is performed by the prospective employer.
 - D. The investigation includes criminal history.
- 9.** Which of the following best describes the purpose of auditing?
- A. It finds the root causes of violation issues.
 - B. It assists investigators in identifying blame for violations.
 - C. It verifies that systems are operating in compliance.
 - D. It searches for hidden unacceptable use of IT resources.
- 10.** Using a RACI matrix, which attribute refers to the party that actually carries out the work?
- A. Responsible
 - B. Accountable
 - C. Consulted
 - D. Informed
- 11.** Which department should take the lead in User Domain compliance accountability?
- A. Information technology
 - B. Information security
 - C. Human resources
 - D. Security
- 12.** A confidentiality agreement sets the expectations of each employee and sets job performance standards.
- A. True
 - B. False
- 13.** Which of the following is a series of individual tasks that users accomplish to comply with one or more goals?
- A. Policy
 - B. Standard
 - C. Procedure
 - D. Guideline
- 14.** Which of the following is a collection of requirements the users must meet?
- A. Policy
 - B. Standard
 - C. Procedure
 - D. Guideline
- 15.** Discretionary access control is based on roles and granted permissions.
- A. True
 - B. False

CHAPTER 9

Compliance Within the Workstation Domain

C

OMPLYING WITH SECURITY-RELATED REGULATIONS, legislation, and other

requirements means ensuring your organization protects the security of your information. In most cases, ensuring information security means ensuring users take appropriate actions and refrain from inappropriate actions. Although the directive seems simple, implementing it can be complex.

If all users were perfect and completely compliant, there wouldn't be a need to consider any further security layers. Remember that users include both authorized and unauthorized users. Attackers fall into the category of unauthorized users. Because users are imperfect and often noncompliant, you must include additional layers of security controls to protect your information's security. The defense-in-depth philosophy provides the best strategy to secure information and remains the basic blueprint for designing security controls. In this chapter, you'll learn how to follow the defense-in-depth strategy to enforce compliance within the Workstation Domain.

Chapter 9 Topics

This chapter covers the following topics and concepts:

- How compliance law requirements relate to business drivers
- Which devices and components are commonly found in the Workstation Domain
- Which access rights and access controls are in the Workstation Domain
- How to maximize C-I-A
- How to manage workstation vulnerability
- How to ensure adherence to documented IT security policies, standards, procedures, and guidelines
- What best practices for Workstation Domain compliance are

Chapter 9 Goals

When you complete this chapter, you will be able to:

- Identify compliance law requirements and business drivers
- Compare how devices and components found in the Workstation Domain contribute to compliance
- Describe methods of ensuring compliance in the Workstation Domain
- Summarize best practices for Workstation Domain compliance

Compliance Law Requirements and Business Drivers

Users generally access information from workstations. This is not always the case, especially as organizations are increasingly using mobile devices such as smartphones and tablets. But workstations are still the most common way for users to view and modify your organization's information. Because workstations provide access to information, they become an attack vector for unauthorized users. It is important that you ensure all items in the Workstation Domain are compliant. [Figure 9-1](#) shows the Workstation Domain in the context of the seven domains in the IT infrastructure.

As with all domains, ensuring compliance in the Workstation Domain satisfies two main purposes:

- **It increases information security**—Because information is a material organizational asset, and in some cases the primary organizational asset, ensuring the security of information equates to protecting the viability of the organization. It is just as important as protecting any other major assets of the organization. A loss of any important asset will likely disrupt your organization's ability to conduct normal operations. It is important to protect your organization's ability to do business.
- **It reduces liability**—If one or more attacks are successful against your organization's information, you might be liable to damages caused to third parties. If information loss or leakage causes damage to other people or organizations and the damage is a result of noncompliance, your organization might be liable for part or all of the damages. At the very least, disclosed successful attacks against your organization can degrade confidence in your commitment to security. An attention to compliance details and strong security can dramatically reduce your organization's exposure to liability claims.

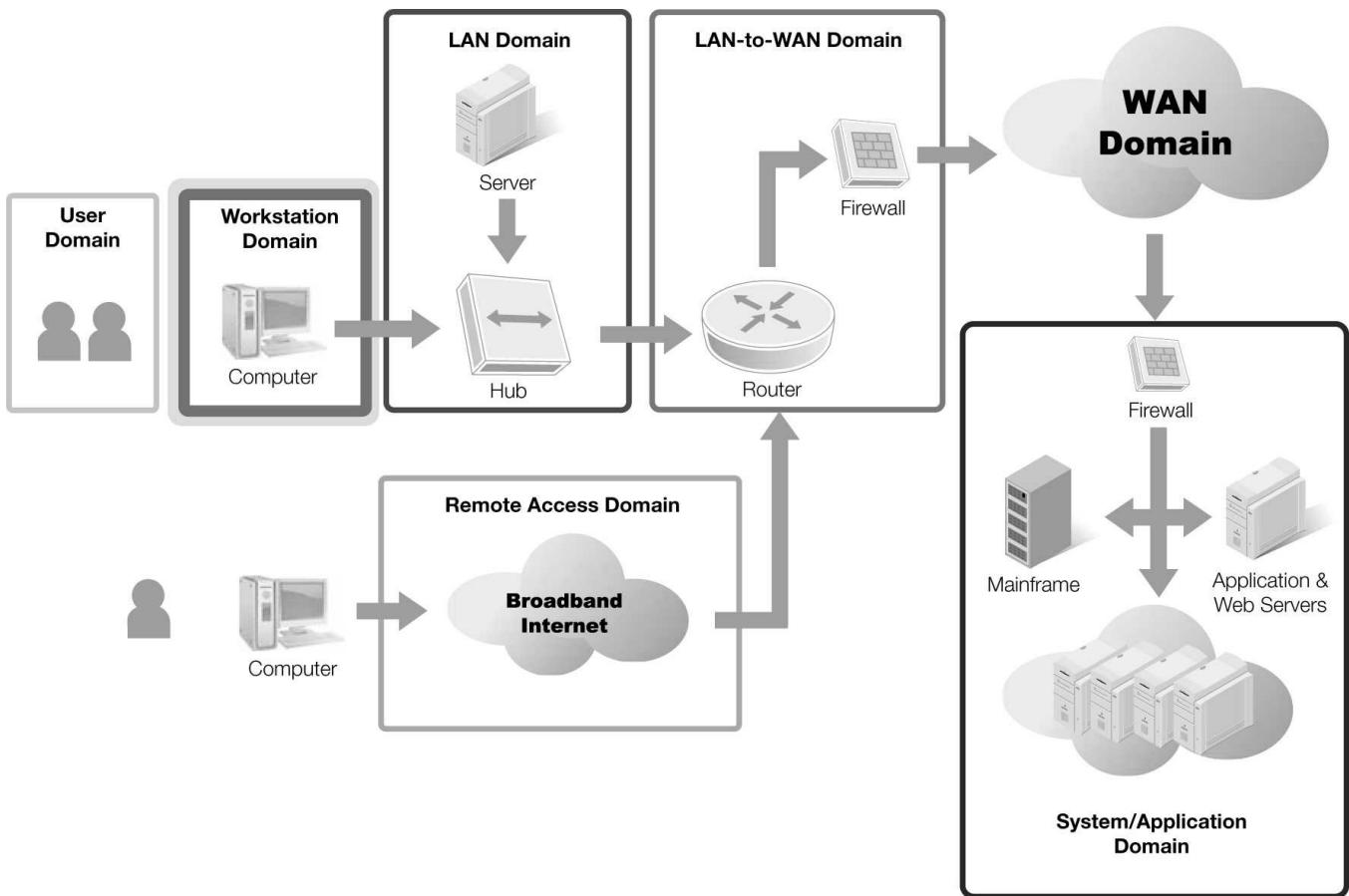


FIGURE 9-1 The Workstation Domain within the seven domains of a typical IT infrastructure.

Due Diligence

Paying attention to compliance can reduce liability in direct and indirect ways. You can think of it in terms of additional insurance. In the context of information security, the term **due diligence** means the ongoing attention and care an organization places on security and compliance. You can reduce your exposure to third-party liability by investing resources in establishing and maintaining compliance. Demonstrating aggressive compliance activities can reduce the liability potential if security incidents result in damages. In short, being compliant looks good in court.

Protecting Private Data

Many recent legislative and regulatory requirements extend the scope of threats to information to include all users. There is no assurance users will be compliant. Organizations need additional layers of controls to protect information because not all threats come from malicious users. Some threats come from simple ignorance. For example, procedural changes might prohibit users from transferring protected files to remote workstations. Properly trained users should not attempt to transfer files to remote workstations, but well-meaning users who are not aware of the new policy might unknowingly violate the policy. The proper way to handle this situation is to do the following:

- Ensure all users receive updated training.
- Place access controls in the Workstation Domain to prohibit inappropriate actions.

You need both types of controls to secure information from all users.

Increased attention to security increases the need to hold employees accountable for

security. Because employees generally have more access to information than other authorized users, they have greater ability to affect the information's security. A greater ability to affect security means you need a greater scope of controls. The most common concern for information security that is reflected in most recent legislation is protecting information privacy. Although information integrity and availability are important, privacy is a primary concern of many regulations. All information system users are accountable for the privacy of the information they access. This puts a greater amount of responsibility and accountability on users.

A solid security strategy should include several types of controls to ensure user compliance. You've already seen some controls in the User Domain. The Workstation Domain is the domain that contains the devices and components to access information. Controlling activities in the Workstation Domain can provide an effective layer of information security. Workstation Domain controls should validate and support controls in other domains. Although controls in the User Domain are important, you need additional controls to ensure compliance with your security policy and any additional security requirements. Controls in the Workstation Domain should work with controls in other domains to ensure a high level of overall compliance.

Implementing Proper Security Controls for the Workstation Domain

Workstation Domain controls are security controls that prohibit, validate, or detect user actions. Users initiate actions in the Workstation Domain that generally involve some stored information. In short, users generally access information using some type of workstation device. It makes sense to place controls at the workstation level to ensure information access is compliant. Proper controls in the Workstation Domain should work with other controls in all domains to enforce compliance without interrupting normal operation.

For example, the Payment Card Industry Data Security Standard (PCI DSS) prohibits merchants from storing the **card verification value (CVV)**. The CVV is a three- or four-digit number that card issuers print on each credit card. The CVV provides additional authentication when rendering payment for online transactions. One control to avoid storing the CVV is to remove any user prompts for the CVV. Although that complies with the PCI DSS data requirement, it also disables the merchant's ability to ask for the CVV to authenticate the transaction. You should not implement this control because it interrupts a necessary business function. Look for another control that balances security and business requirements.

E-mail Policy

Another example of multiple layers of controls is an e-mail policy. Every organization should have a policy on appropriate use of e-mail at work. E-mail messages can contain private information that employees can easily disclose. It is important that your employees carefully control destinations for private information to avoid unintended disclosure. Creating controls in multiple domains will help minimize private information disclosure. Controls may include security awareness training in the User Domain, e-mail client filters and rules in the Workstation Domain, and e-mail server rules and filters in other domains. Once again, multiple layers of controls in different domains greatly reduce the risk of disclosing private information and exposing your organization to potential liability.

A good strategy to identify the best Workstation Domain controls is to start with your security policy. Identify any requirements that directly relate to workstation components and

create appropriate controls. The task of identifying controls is much easier if you consult ISO/EIC 27001, which provides a concise list of security controls. For more in-depth understanding of every control, ISO 27002 is the best reference. After you have a list of potential controls, compare your list to the User Domain controls. The Workstation Domain controls should complement controls in other domains, but should specifically support User Domain controls.

A good way to enforce this approach is to create controls of different types for different domains. For example, suppose you want to enforce your password policy. You may have an administrative control in the User Domain that mandates user training on proper passwords. A good Workstation Domain control would be to enforce complex passwords on all workstations. This would be a technical control that enforces strong passwords by prohibiting weak passwords. Users should already know how to create strong passwords from their training. However, forcing strong passwords using a Workstation Domain control ensures that users follow the requirements. Once these controls are put into practice, they serve as countermeasures for the organization. Countermeasures are the controls you put in place to mitigate a risk. This is another example of a defense-in-depth strategy.

 **NOTE**

Your Workstation Domain controls should not just duplicate User Domain controls, but should provide a second level of assurance.

Devices and Components Commonly Found in the Workstation Domain

The Workstation Domain connects users to local resources. Remote users are covered in the Remote Access Domain. The Workstation Domain includes all local resources that support user functionality and allow users to interact with your information system. In some cases, Workstation Domain items collect and present information as well as process that information. In other cases, processing occurs in another domain. In either case, users use the Workstation Domain to interact with the rest of your environment, including your data. Each type of device or component in the Workstation Domain presents potential vulnerabilities and security challenges. It is important that you carefully consider each type of component when you design Workstation Domain controls. [Figure 9-2](#) shows the most common devices and components you'll find in the Workstation Domain.



FIGURE 9-2 Devices and components in the Workstation Domain.

Uninterruptible Power Supplies

An **uninterruptible power supply (UPS)** provides continuous usable power to one or more devices. Some UPS models also provide the ability to protect data connections from power surges that could damage computers or other hardware. A UPS can protect many types of devices and may exist in several domains. Their primary purpose is to support the availability of Workstation Domain devices. UPS devices generally provide several types of protection, including the following:

- **Continuous power**—A primary purpose of a UPS is an integrated battery that provides power to connected devices when the AC power fails. When the AC power fails, or even falls below usable voltage, the UPS automatically switches to its battery to provide uninterrupted power to any devices connected to the UPS. This feature allows the connected devices to continue operating normally during power outages. Because the backup power depends on the UPS battery, the duration of the power is limited—generally around 30 minutes. Although larger UPSs include backup power generators that can provide power for extended periods of time, devices in the Workstation Domain generally do not require such measures. The ability to survive short duration power outages is generally sufficient.
- **Surge protection**—Nearly all UPSs condition the power supplied to connected devices. Conditioned power means that any voltage surges are removed before providing power to devices. This surge-filtering capability protects connected devices from potential damage from high voltage. Some UPSs include network connectors that protect networking connections from power surges as well as power connections.
- **Structured shutdown**—Many UPSs provide the ability to establish a communications connection to a primary computer. This connection allows the UPS to send a shutdown request to the computer when the UPS power is in danger of running out. When a power outage duration approaches the UPS power limit, the UPS can alert the computer and allow it time to shut down gracefully. This ability protects data integrity by avoiding uncontrolled shutdowns that could cause damage to open data files.

Desktop Computers

Desktop computers have historically been the most common type of Workstation Domain device. That trend is rapidly giving way to more mobile computing. Desktop computers are designed to be stationary and are often physically connected to an organization's network to share information and devices. Because they are commonly connected to other network resources, it is important to carefully control access to these computers.

Most desktop computers have substantial local processing power and are often used to locally create and manage data. Although this ability can reduce the workload on other domain devices, it can also lead to data leakage. Users who are comfortable working with information locally on a desktop computer might not be diligent about backing up the information or perhaps about protecting the information.

Desktop computers have grown in power and storage capacity in recent years to the degree that they rival the capabilities of some server computers. This increase in power encourages users to install more and more software on their desktop computers. Allowing unsupervised software installations can lead to desktop computers that are difficult to support or even dangerous to your organization. Many computer problems relate to conflicts between programs that are competing for resources. Allowing users to install unapproved programs increases the likelihood of conflicts with approved programs.

Desktop Computers and Privacy

Many users think of their desk environment and desktop computers as private areas. When conducting security assessments, it is a common practice to examine desktop environments for confidential information. Far too many users write their passwords on sticky notes and place them on or around the computer monitor. Another favorite place to "hide" passwords is under the keyboard. This common practice punctuates two warnings:

- Don't make compliance with your password policy so difficult that users have to write down their passwords.
- Pay attention to physical controls that keep unauthorized people away from authorized users' desks.

A lack of desktop computer control also increases the likelihood that users will unknowingly install malicious software. A desktop computer with malware is not only a threat to locally stored information but also to all other devices connected to your network. It is important to understand the risks of allowing too much user freedom and implement the appropriate controls to protect your organization.

Laptops/Tablets/Smartphones

As computers shrink in size and grow in capabilities, several new classes of computers now rival the desktop as the most popular type of workstation. Laptop computers are generally the larger, more powerful class of portable computers. Laptop computers can do nearly everything a desktop computer can do while maintaining a small enough profile to be very portable. Most laptop computers fit easily into briefcase-size bags and backpacks.

Tablet devices and smartphones have gained greater widespread capabilities and use. They are smaller and lighter than laptop computers. Their smaller size and lighter weight means that they generally have fewer hardware options and limited capabilities. Tablets and smartphones are generally designed to act as access devices to network devices and don't provide much local storage. Although they lack much local storage space, they still pose risks

because of their support for network access.

As with desktop computers, it is important to control access to network resources and the ability to install unauthorized software. In fact, the need to control portable computers is more important than with desktop computers. The portable nature of laptops, tablets, and smartphones means these computers are likely transported and used at locations physically outside of your organization. In most cases, users connect portable computers to other networks when they are away from your organization's building. Connecting to unprotected networks can be extremely dangerous. Users can pick up infected programs when connected to other networks and then introduce them the next time they connect to your network. Your security policy should include specific standards for using portable computers to connect to your networks.

Local Printers

A local printer is any printer connected directly to a computer. Local printers aren't shared by multiple users. Because these printers aren't connected to your organization's network, they aren't controlled from a central location. This means local users can print anything they want. Allowing users to access local printers without any controls can lead to several types of issues, including the following:

- **Personal use of the organization's resources**—Users can print any files to local printers. This can include personal information that might violate the acceptable use policy.
- **Disclosure of private information**—Users can print files with little or no control over content. There is always the chance that printed documents could end up in the wrong person's hands.
- **Printer buffer access**—Most printers retain copies of recently printed documents. It is not difficult to get a printer to reprint previously printed documents. It can be difficult to control this behavior on local printers.

Minimize local printer use in your organization. Printers should generally be networked and managed from a central location in another IT domain.

Modems and Wireless Access Points

Modems and wireless access points can pose serious threats to organizations. At first glance, they don't seem too dangerous, but they can provide damaging backdoor entryways into your network. These devices do have a place in a secure environment but not in the Workstation Domain. Modems provide a connection to another computer or network and belong in another domain where you can control them in a way that protects your network. Wireless access points provide a wireless connection to the network or computer systems. Like modems, they belong where they can be more closely controlled. Modems and access points connected to Workstation Domain devices are almost always uncontrolled and installed to bypass network access controls.



WARNING

As innocent as it might seem, simply connecting an analog modem can potentially compromise your network. It is important that you search for rogue modems and ensure you either eliminate or carefully control each modem in the Workstation Domain.

Although many users consider these devices to be harmless, they can be valuable tools for attackers. Many attackers still employ an old technique called **wardialing** for modems and **wardriving** for wireless access points. Wardialing is instructing a computer to dial many telephone numbers, looking for modems on the other end. The wardialing computer records any modems it finds for later analysis. Each modem that answers a wardialing computer is a potential target. Attackers will dial identified numbers and attempt to access the computer on the other end. Unauthorized modems are rarely secured well and are known to be fairly soft targets. The attacker attempts to access the computer to which the modem is attached and then moves on to attack the organization's network. Wardriving is similar. It is used to quickly find wireless networks. This technique gets its name from the act of driving around in a motor vehicle with a mobile computer and special software that locates wireless networks.

Fixed Hard Disk Drives

Virtually all general-purpose computers have at least one internal, fixed hard drive. Computers primarily use fixed hard drives to store the computer's operating system as well as application programs and data. Some leading-edge or special-purpose computers use solid state memory to store programs or information, but most of today's computers use regular hard disk drives. Disk drives store files that contain data, instructions, or both.

Privacy laws and regulations address both types of file contents. Compliance with different requirements often means restricting how you access certain types of information or how you must store information. For example, under the Health Insurance Portability and Accountability Act (HIPAA), you must protect all private medical information from unauthorized disclosure. That often means using centralized storage with carefully monitored access and storage controls. You implement centralized storage in another IT domain, not in the Workstation Domain. Continuing the example, assume you use your workstation to access private medical information. You decide to copy the information into a document and store it locally on your workstation while you edit the information. The decision to store the information locally potentially just violated HIPAA. The problem is that you have just placed private medical information in an area that unauthorized users can potentially access.

You must carefully control what devices in the Workstation Domain can do. The good news is that you do have some control when Workstation Domain devices reach across domains. Storing information from another domain is only one issue. You also need to control files stored on the hard disk that originate outside your organization's IT infrastructure. Outside programs and files often result from activity while you are connected to another network. In most cases, Internet access provides the inbound path for unwelcome files. Malicious files and software can infect unprotected computers and then spread to other computers and devices in your organization. Controls in the Workstation Domain for disk drive access can help prevent infections and protect the rest of your network.

Removable Storage Devices

One last category in the Workstation Domain includes devices you connect to computers as you need them. You use most of the devices in this category to store files to transport to another computer. These devices include the following:

- Removable hard disk drives
- Universal serial bus (USB) flash drives
- Removable CD-ROM and DVD drives

- Removable tape drives

There are other removable storage devices, but these are the most common. In fact, the most common devices are USB flash drives. These drives are compact, are easily available, and can rival internal storage drives in terms of capacity.

Because you can transport removable media easily and connect it to other computers, it is important that you control the files you transfer both to and from any such devices. In general, you should control two types of transfers:

- **Information you copy to a removable device to ensure you protect data privacy**—This type of control keeps you from divulging private information.
- **Data you copy from a removable device to block malicious code or data**—This type of control prevents the rest of your environment from introducing malicious code.

Understanding the devices and components in the Workstation Domain is the first step to establishing controls to secure this domain. The next step is to understand data and device access controls. You'll learn about Workstation Domain access rights and controls in the next section.

Access Rights and Access Controls in the Workstation Domain

You learned in the previous sections how important it is to implement the correct controls in the Workstation Domain. Proper security controls limit access to objects based on a user's identity. Access control methods may be based on the permissions granted to a user or group, or they may be based on a user's security clearance. Either way, access rights start with knowing which user requests access to an object and what the user's identity permits him or her to do.

Most computers require you to log on before you can access any resources on the computer. Even systems set up to automatically log on are actually logging on to a predefined user account. The first step in logging on is to provide a user ID or username. Providing user credentials or claiming to be a specific user is called **identification**. Simply identifying yourself is not enough. If all you have to do is claim to be a user, anyone can claim to be a system administrator and gain permission to carry out potentially harmful actions. Operating systems require users to follow the identification step with authentication. **Authentication** is the process of providing additional credentials that match the user ID or username. Only the operating system and the real user should know the authentication credentials. The most common authentication credential is the password. Other options include security tokens and biometric characteristics. When you provide the correct user ID and authentication credentials, you are logged on to your user account.

As the operating system logs you on, it looks up security **authorization** information and grants you access permissions based on your identity. (Authorization refers to the access rights allowed.) There are two main approaches for authorizing users to access objects. Both approaches evaluate whether a user, also called a **subject**, has the permission to access some resource, also called an **object**. Access objects can be files, directories, printers, or any resource. There are other methods as well, but two methods are the most common ones you'll encounter.

The first access method uses **access control lists (ACLs)**, which are lists of access **permissions** that define what each user or security group can do to each object. Each object uses ACLs or permissions to define which users can access it. The object's **owner** can grant

access permissions to any desired user or group. Because granting access is at the owner's discretion, this type of access control is called discretionary access control (DAC).

The second type of access control is not based on specific permissions but on the user's security clearance and the object's classification. Organizations that use this type of access control assign a specific classification to each object. Security classifications used by the U.S. government, for example, include Top Secret, Secret, Confidential, and Unclassified. Other governments and nongovernmental organizations use slightly different classifications but most classification schemes are similar. Each user receives a security clearance that corresponds to one of the classifications in use. The operating system grants access to objects based on a user's security clearance and the requested object's classification. For example, a user with a Secret clearance can access Secret, Confidential, and Unclassified objects but cannot access Top Secret objects. Because there is no discretion involved in granting access, this access method is called mandatory access control (MAC).

Authentication Types

There are three main types of authentication credentials—**Type I (what you know)**, **Type II (what you have)**, and **Type III (what you are)**. The credentials are described as follows:

- **Type I authentication (what you know)**—This is information only a valid user knows. The most common examples of Type I authentication are a password or personal identification number (PIN).
- **Type II authentication (what you have)**—This is a physical object that contains identity information, such as a token, card, or other device.
- **Type III authentication (what you are)**—This is a physical characteristic (biometric), such as a fingerprint, handprint, or retina characteristic.

Type II authentication is generally stronger than Type I, and Type III is generally stronger than either Type I or Type II. You can make the authentication process even stronger by using more than one type at the same time. Using two types of authentication is called **two-factor authentication** and using more than two types is called **multifactor authentication**. Using more than a single authentication type strengthens the process by making it more difficult to impersonate a valid user.

Regardless of the access control method you use, the end result is the ability to restrict access to objects by user account. Access control methods enable you to define an access control strategy that allows you to define controls to support your security policy.

Maximizing C-I-A

The overall purpose of compliance requirements is to enforce the basic pillars or tenets of security. Although some compliance requirements might seem to be unnecessary, they all should work together to support the **C-I-A** properties of secure systems. As a review, here are the three tenets of information security:

FYI

C-I-A stands for confidentiality, integrity, and availability. The term is also known as A-I-C (availability, integrity, and confidentiality). Some information systems security professionals refer to the tenets as the **C-I-A triad** to avoid confusion with the U.S. Central Intelligence Agency, commonly referred to as the CIA.

- **Confidentiality**—Assurance that the information cannot be accessed or viewed by unauthorized users
- **Integrity**—Assurance that the information cannot be changed by unauthorized users
- **Availability**—Assurance that the information is available to authorized users in an acceptable time frame when the information is requested

[Figure 9-3](#) shows the C-I-A triad.

Notice that a central theme of the C-I-A properties is the difference between authorized and unauthorized users. The identification, authentication, and authorization process you learned about in the previous section provides the foundation for securing information in any domain. Maximizing the C-I-A properties is all about ensuring authorized users can access trusted data and unauthorized users can't.

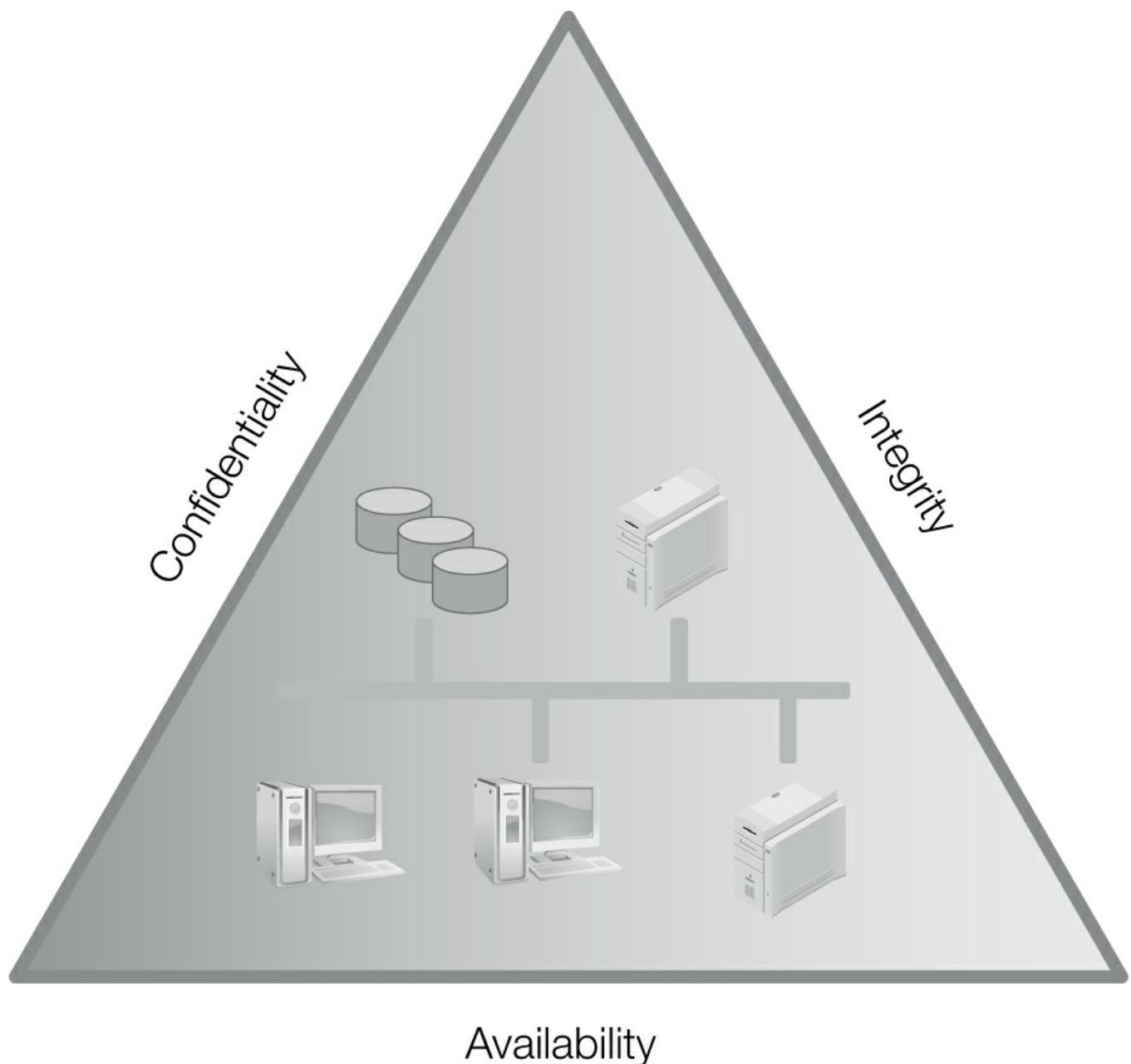


FIGURE 9-3 C-I-A triad.

Maximizing Availability

Secure information serves the purpose for which it was created. Secure information must be available when the information is requested. This requirement means that information should be available during normal processing, but also during and after unusual events. Unusual events include minor events such as short-term power outages up to major disruptions and disasters. There are two main areas in the Workstation Domain that can affect availability:

- Surviving power outages
- Executing a solid backup and recovery strategy

You should address each area when you create Workstation Domain controls.

Surviving Power Outages

The easiest way to ensure your computers and devices can continue operating in the event of a power outage is by using a UPS. The first step in implementing the right UPS is to list each of the computers and devices you want to protect. Consider any supporting devices you'll need along with computers. For example, if you want to be able to stay online during a power outage, you'll need to ensure you connect any network access devices to the UPS as well. Once you have a list of all devices, add up the power requirements for all devices you'll attach to the UPS. Then, search UPS manufacturers for a UPS that will satisfy your service and power requirements. An Internet search is a good place to start.

Backup and Recovery Strategy

A UPS is fine to keep your computers up and running when the power goes out for a few minutes, but what do you do in case of a disaster? What happens to the programs and data on your Workstation Domain computers if a fire in your office destroys the computers? Fire is only one type of disaster your computers might encounter. Information that burns up in a fire or is destroyed in a flood is not available when you need it. Because the information isn't available in this situation, it isn't very secure.

technical TIP

UPS devices come in many price ranges and provide varying levels of service. Lower-cost UPSs simply switch over to a battery when you lose full power. Higher-cost UPSs provide line conditioning and handle brownouts and blackouts in different ways. Higher-priced UPSs also tend to provide backup power for longer periods of time. Don't just shop for price—carefully examine the features on several different UPS models before purchasing one.

You must have a plan to periodically create secondary copies of your important information. This secondary copy is often called a backup. Creating a backup copy of information is important, but is only one step in a plan to ensure availability. The real key to ensuring availability is to have a plan for restoring your information to the state in which it existed before a disaster. Your backup and recovery strategy should include the following:

- **Backup plan**—This is a plan to create frequent backup copies of important files. This plan includes identifying the files you need to back up, deciding on which backup utility to use, and setting a schedule for creating backups.
- **Safe media storage plan**—This is a plan to protect your backup copies. This plan

includes procedures for transporting backup media to a protected location. In most cases, you want to keep copies of your important information in remote locations to keep them safe from disasters that might affect your primary office. Consider keeping backup copies far enough away from your primary office that a disaster won't affect them. For example, a flood or earthquake can affect a large area. You may need to store backup copies far away, even in a different geographic region.

- **Restore plan**—This is a plan to use the backup media to restore your environment to working order. This is often the plan people overlook. You need backups, but you also need a plan that tells how to use the backups to build a working system.

The most important aspect of ensuring availability is to plan for situations that might disrupt your organization's activities and know what to do in those instances. Plan ahead and you won't likely be caught not knowing what to do when a disaster strikes.

Maximizing Integrity

The term **malware** refers to a collection of different types of software that share the goal of infiltrating a computer and making it do something. In many cases, malware does something undesired and operates without the explicit consent of the owner. This is not always the case, however. Some types of malware are downloaded and installed with the owner's full knowledge. Malware can be loosely divided into two main categories: programs that spread or infect and programs that hide.

Programs that spread or infect actively attempt to copy themselves to other computers. Their main purpose is to carry out instructions on new targets. Malware of this type includes the following:

- **Virus**—A software program that attaches itself to or copies itself into another program for the purpose of causing the computer to follow instructions that were not intended by the original program developer is called a **virus**.
- **Worm**—A self-contained program that replicates and sends copies of itself to other computers, generally across a network is called a **worm**.

Other malware hides in the computer to carry out its instructions while avoiding detection. Malware that tends to hide includes the following:

- **Trojan horse**—Software that either hides or masquerades as a useful or benign program is called a **Trojan horse**.
- **Rootkit**—Software that modifies or replaces one or more existing programs to hide the fact that a computer has been compromised is called a **rootkit**.
- **Spyware**—Software that covertly collects information without the user's knowledge or permission is called **spyware**.

Understanding these five basic types of malware and how to protect your systems from them is important to a solid security plan. You install anti-malware software to protect Workstation Domain computers. There are many anti-malware software products from which you can choose. Carefully review suppliers and their products for costs, functionality, and support. The best place to look for specific anti-malware for your operating system is the Internet. Use an Internet search engine to search for “antivirus software” and “antispyware software.”

After you decide on one or more anti-malware products, you must develop procedures to ensure the products and their signature databases are kept up to date. With new viruses,

worms, and Trojan horses being released every day, it is important that your software be kept current to recognize as many new threats as possible. Up-to-date anti-malware software can help make your Workstation Domain computers more secure and able to ensure information integrity.

Maximizing Confidentiality

Because Workstation Domain computers may store sensitive or private information, it is important to protect the information from disclosure to unauthorized users. Two methods are commonly used to protect information confidentiality. **Access controls** can help ensure that unauthorized users cannot access protected objects. The easiest way to deny access to anyone other than authorized users is through access permissions. If you grant read and write access only to authorized users, the operating system ensures the information's confidentiality. Regardless of your choice of access control methods, you can assign user accounts to enforce confidentiality.

There is a drawback to using operating system access controls. It is possible for an attacker with physical access to a computer to boot the computer using alternate boot media. Most Workstation Domain computers have USB ports and CD/DVD drives. Either of these can support booting. If you insert a bootable CD/DVD or USB drive, many computers will boot from the alternate devices instead of the internal disk drive.

Booting from alternate boot media makes it easy to access files directly from the disk. If you boot from a CD/DVD or USB drive, you can bypass the operating system access controls and access any files you want. So, operating system access controls don't fully protect the confidentiality of your information. **To protect private information at all times, you need to protect it even when the operating system isn't running. Only encryption provides that much protection.**

technical TIP

Whether a particular computer will boot from the CD/DVD drive or USB device before the internal disk drive depends on that computer's complementary metal-oxide semiconductor (CMOS) configuration. Most computers allow you to enter a setup mode to alter CMOS settings, including the device boot order, by pressing the Delete key, F2, or F11 early in the boot process. Specific keys and options differ between computer manufacturers.

Encrypting data makes it unreadable to everyone without the decryption key. You can encrypt all sensitive information and provide the decryption key only to authorized users. Attackers can still boot your computer using alternate media; however, they will see only encrypted files and will be unable to read their contents.

TIP

Each operating system supports encryption a little differently and some need third-party software to encrypt folders or entire drives. Explore how your operating system supports encryption and use it to secure private information.

Workstation Vulnerability Management

Because Workstation Domain computers and devices are commonplace and plentiful, they make good attack targets. Workstations generally are not located in areas that are as secure as devices in some other domains. They also exist in sufficient numbers that there is a high probability of finding vulnerable computers.

Although you can't make every computer and device totally secure, you can make them secure enough to frustrate all but the most determined attackers. In general, your computer environment doesn't have to be totally secure—just more secure than the attacker's next target. If you can get an attacker to give up and go on to another target, you have been successful.

Operating System Patch Management

One of the first attack activities is to identify a target machine's operating system and look for any known vulnerabilities. There are multiple methods attackers use to identify, or fingerprint, a target machine. **Fingerprinting** a computer means identifying the operating system and general configuration of a computer. Attackers will fingerprint a computer and use that information to identify known vulnerabilities for that operating system version.

It is important to keep your operating system up to date and patched. Applying the latest security patches eliminates many of the vulnerabilities attackers are looking for when planning attacks.



TIP
Explore options for automatically acquiring and applying operating system patches. Automatic updates can reduce the administrative workload by ensuring the latest patches get installed on Workstation Domain computers.

Application Software Patch Management

After fingerprinting, a computer attacker scans target computers for information on resident applications. Just like operating systems, applications may contain security vulnerabilities and provide attackers with an opportunity to compromise a computer. It is important to keep your applications up to date as well as your operating system.

Develop a plan to keep all applications up to date. Each application's provider may approach the update process differently. Some vendors provide automatic update notifications and others report updates only when directly queried. Know the update policy for each of your vendors. Create procedures to ensure you update all applications with the latest security patches. Keeping applications current will reduce the number of vulnerabilities on your computers and make it harder for attackers to succeed.

Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines

Workstation Domain computers and devices are often the most visible components to users. The majority of users access an organization's applications and information using Workstation Domain computers. That means Workstation Domain computers and devices tend to interact with users a lot. Many security issues result from user errors and can be addressed with proper training. However, training can address only some of the security

issues related to users. Eventually, an untrained, unmotivated, or careless user will violate security policy and will perform an action that causes a security incident. The incident might be large or it might be very small and unimportant. Regardless, it is important to employ multiple layers of controls to ensure security does not rely on any single control. Even organizations with very effective training programs encounter problems that users create.

A solid security policy should define multiple layers of controls working together to keep your information secure. Your security policy should direct security activities and state standards that maintain compliance with legislation, regulations, and any other requirements. Following procedures and guidelines should always result in fulfilling your security policy as well as any other organizational policies.

FYI

How your organization implements its security policy can follow an auditing framework. For example, if the organization follows the Committee of Sponsoring Organizations (COSO) or Control Objectives for Information and Related Technology (COBIT) auditing framework, the process of implementing the security policy and guidelines can be more aligned to that framework. This helps an organization compare “apples to apples” while auditing. Similarly, if an organization relies on outsourced services, it can make use of auditing standard SSAE 16 to best assess the provider.

Periodically, an organization should assess its adherence. To accomplish this, an organization can perform a gap analysis to determine what holes might exist in how it enforces the security policy. Specifically, the organization can compare the present situation with the desired situation. Once identified, the gap between is used to create actionable tasks.

Procedures define the steps necessary to fulfill the intent of the security policy. The Workstation Domain procedures can cover many aspects of maintaining computers and devices, but should include the following:

- Change password procedure
- Logon/logoff procedure
- Backup procedure, including handling backup media
- Recovery procedure
- Update operating system and application software procedure
- Maintain private data procedure
- Malware alert procedure
- Grant/deny object access procedure

Procedures provide the step-by-step instructions for fulfilling the security policy but cannot include every variable. Sometimes, you have to make decisions based on the information at hand. In these cases, guidelines can help you make decisions that still comply with your security policy and any other organizational policies. Workstation Domain guidelines can include the following:

- Strong password guideline
- Document-naming guideline
- Printer use guideline
- Software installation guideline
- Handling backup media guideline

- Internet use guideline

Use operating system controls whenever possible to enforce Workstation Domain policies. These controls will not fulfill all aspects of the security policy, but they will provide a solid foundation for ensuring your information's security. Controls you will find in most current operating systems include the following:

- General object access permissions
- Shared object access permissions
- Private object access permissions
- Printer permissions
- Audit logging settings
- Authentication requirements
- User rights

Taken together, policies, procedures, and guidelines provide the instructions and limits that enable your users to comply with your security policy when using components of the Workstation Domain. Even though you design and deploy controls to limit user actions, you still should deploy additional controls to detect noncompliant behavior. Use your operating system's access audit logging features to keep log files of interesting object access requests. Carefully consider which objects you want to audit. Auditing access requests for all objects will slow your computers down and waste disk space. Identify the objects that contain sensitive or private information and enable audit logging for those objects.

 **NOTE**

Reviewing audit logs will show how users are using Workstation Domain computers and devices. The audit process uses these log files to validate that usage complies with your security policy.

A second useful technique during an audit is to compare a snapshot, or baseline, of a computer or device as it currently appears with a baseline from a previous point in time. Any differences between baselines could indicate unintended changes and possible vulnerabilities. Your audit plan should include procedures to create periodic baselines that you can use to detect unwanted changes to your computers and devices. A baseline can contain many types of information, but should include the following:

- Users and settings
- Groups and members
- File list with access permissions
- Access control lists
- Configuration settings for important applications and services
- Installed application list
- Startup/shutdown and logon scripts or batch files
- Network adapters and configuration

You should include any other information that describes the configuration of a specific computer. One of the easiest ways to create baselines is to include the commands that list the

desired information in a script or batch file. You can compare saved output from any baseline to see configuration changes between snapshots. Creating periodic baselines supports the overall audit process to ensure compliance with stated security goals.

Best Practices for Workstation Domain Compliance

Workstation Domain computers and devices provide local computing resources and often provide initial access into your organization's shared resources. It is important to maintain a secure Workstation Domain for the security of the locally stored information as well as to keep other domains secure. Allowing Workstation Domain components to be unsecure increases the vulnerability for other domains you access from workstations.

There are many strategies for keeping the Workstation Domain secure. Each organization should customize its Workstation Domain policies, procedures, and guidelines for its specific set of requirements. If the organization is a federal entity, compliance with the NIST 800-53 standard is mandatory. The assessment of those controls is covered in depth in guideline NIST 800-53a.

Here are general guidelines and best practices to attain and maintain compliance within the Workstation Domain:

- Require unique user accounts for each person. Do not allow multiple people to use the same user account.
- Require strong passwords and train users on the importance of keeping passwords private. Require users to change passwords at a specified interval, such as every six months.
- If one person performs duties of several roles, create a unique user account for each role.
- If using DAC, assign object permissions for all shared objects to grant access only to necessary subjects.
- If using MAC, establish simple standards for assigning security classifications to objects.
- Create a backup schedule that minimizes the amount of work that would be lost if a disaster destroyed the computer just before the next backup.
- Document procedures for labeling, transporting, storing, and reusing backup media.
- Document the steps necessary to restore your system from a backup after data loss.
- Test your recovery procedure at least every six months.
- Test the power outage operation of your UPS at least monthly.
- Conduct informal monthly audits that include creating monthly baselines.
- Check for anti-malware software and signature database updates daily.
- Scan for operating system and application updates at least weekly.
- Audit users, groups, and access permissions/data classification at least quarterly.

Although this list of best practices is not exhaustive, it is a good foundation to keep Workstation Domain computers and devices secure.



CHAPTER SUMMARY

The Workstation Domain contains computers and devices that provide the primary interface for most users. Many information system users access local and networked resources from computers in the Workstation Domain. Securing components in this domain has a dual effect of securing information on individual workstations and helping to avoid introducing vulnerabilities into the organization's network.

You learned about the importance of access controls, maximizing the C-I-A properties of security, and backing up and restoring information. You also learned strategies for staying malware-free and keeping the operating system and application software up to date. The tasks necessary to keep the Workstation Domain secure cover several areas and require diligence. The result is a domain that supports your organization's business functions and keeps your information secure.



KEY CONCEPTS AND TERMS

Access control lists (ACLs)
Authentication
Authorization
Card verification value (CVV)
C-I-A
Due diligence
Fingerprinting
Identification
Malware
Multifactor authentication
Object
Owner
Permissions
Rootkit
Spyware
Subject
Trojan horse
Two-factor authentication
Type I authentication (what you know)
Type II authentication (what you have)
Type III authentication (what you are)
Uninterruptible power supply (UPS)
Virus
Wardialing
Wardriving
Worm



CHAPTER 9 ASSESSMENT

1. _____ means the ongoing attention and care an organization places on security and compliance.
2. PCI DSS allows merchants to store the CVV number.

 - A. True
 - B. False
3. Which of the following choices protect your system from users transferring private data files from a server to a workstation? (Select two.)

 - A. Increase the frequency of object access audits.
 - B. Deliver current security policy training.
 - C. Place access control to prohibit inappropriate actions.
 - D. Enable access auditing for all private data files.
4. Some attackers use the process of _____ to find modems that may be used to attack a computer.
5. Which security-related act requires organizations to protect all personal medical information?

 - A. HIPAA
 - B. GLBA
 - C. SOX
 - D. SCM
6. Which of the following is the process of verifying credentials of a specific user?

 - A. Authorization
 - B. Identification
 - C. Authentication
 - D. Revocation
7. Which of the following is the process of providing additional private credentials that match the user ID or username?

 - A. Authorization
 - B. Identification
 - C. Authentication
 - D. Revocation
8. Which access control method is based on granting permissions?

 - A. DAC
 - B. MAC
 - C. RBAC
 - D. OAC
9. The _____ property of the C-I-A triad provides the assurance the information cannot be changed by unauthorized users.
10. What are the types of malware? (Select two.)

 - A. Programs that actively spread or infect
 - B. Programs that slow down data transfer
 - C. Programs that cause damage
 - D. Programs that hide
11. A _____ is a type of malware that is a self-contained program that replicates and sends copies of itself to other computers.

CHAPTER 10

Compliance Within the LAN Domain

S

TANDALONE COMPUTERS can be very useful, but they are far more effective when

they are able to communicate with one another. Computers that can communicate and exchange information have the ability to assume specific roles that make your organization's computing environment more efficient and effective. Unfortunately, connecting computers also makes accessing your organization's information easier for both authorized and unauthorized users. That means you have to be diligent to ensure the confidentiality, integrity, and availability of your data.

In this chapter, you'll learn about techniques many organizations use to ensure information is secure within locally connected computers. The controls and techniques that can help meet compliance requirements are also explained. You'll learn how to connect computers together without risking the organization's information due to loss, alteration, or disclosure.

Chapter 10 Topics

This chapter covers the following topics and concepts:

- How compliance law requirements relate to business drivers
- Which devices and components are commonly found in the LAN Domain
- What LAN traffic and performance monitoring and analysis are
- What LAN configuration and change management are
- Which LAN management tools and systems are commonly used
- What access rights and access controls in the LAN Domain are
- How to maximize C-I-A
- How to manage the vulnerability of LAN components
- How to ensure adherence to documented IT security policies, standards, procedures, and guidelines
- What best practices for LAN Domain compliance are

Chapter 10 Goals

When you complete this chapter, you will be able to:

- Examine compliance law requirements and business drivers
- Compare how devices and components found in the LAN Domain contribute to compliance
- Describe methods of ensuring compliance in the LAN Domain
- Summarize best practices for LAN Domain compliance

Compliance Law Requirements and Business Drivers

Users generally use their workstations to access other resources that are connected to an organization's local area network (LAN). A LAN is a network that covers a small physical area, such as an office or building. Resources that are connected to a LAN are potentially available to users using workstations also connected to the LAN. Because LANs increase the number of potential users that can access any resource on the LAN, it becomes even more important to control access to resources and monitor LAN activity to ensure controls are doing their job. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires controls to protect credit card information. The Health Insurance Portability and Accountability Act (HIPAA) requires controls on personal health information. As LANs become more and more useful to authorized users and attackers, it is more important than ever to ensure compliance within the LAN Domain. [Figure 10-1](#) shows the LAN Domain in the context of the seven domains in the IT infrastructure.

Organizations rely on networked resources more than ever in today's environments. LANs make it possible to share expensive resources, such as color printers and high-performance disk subsystems. In fact, LANs enable more efficiency in critical business functions by supporting faster information transfer and resource sharing. These benefits often result in direct cost reductions and productivity increases. Organizations rely on LAN resources to maintain cost-efficient operations. Protecting the LAN-based services directly affects costs and efficiency. A solid security policy that includes compliance with all appropriate requirements should support efficient and cost-effective operation. Implementing the controls necessary to support your security policy in the LAN Domain makes your organization more secure and more effective.

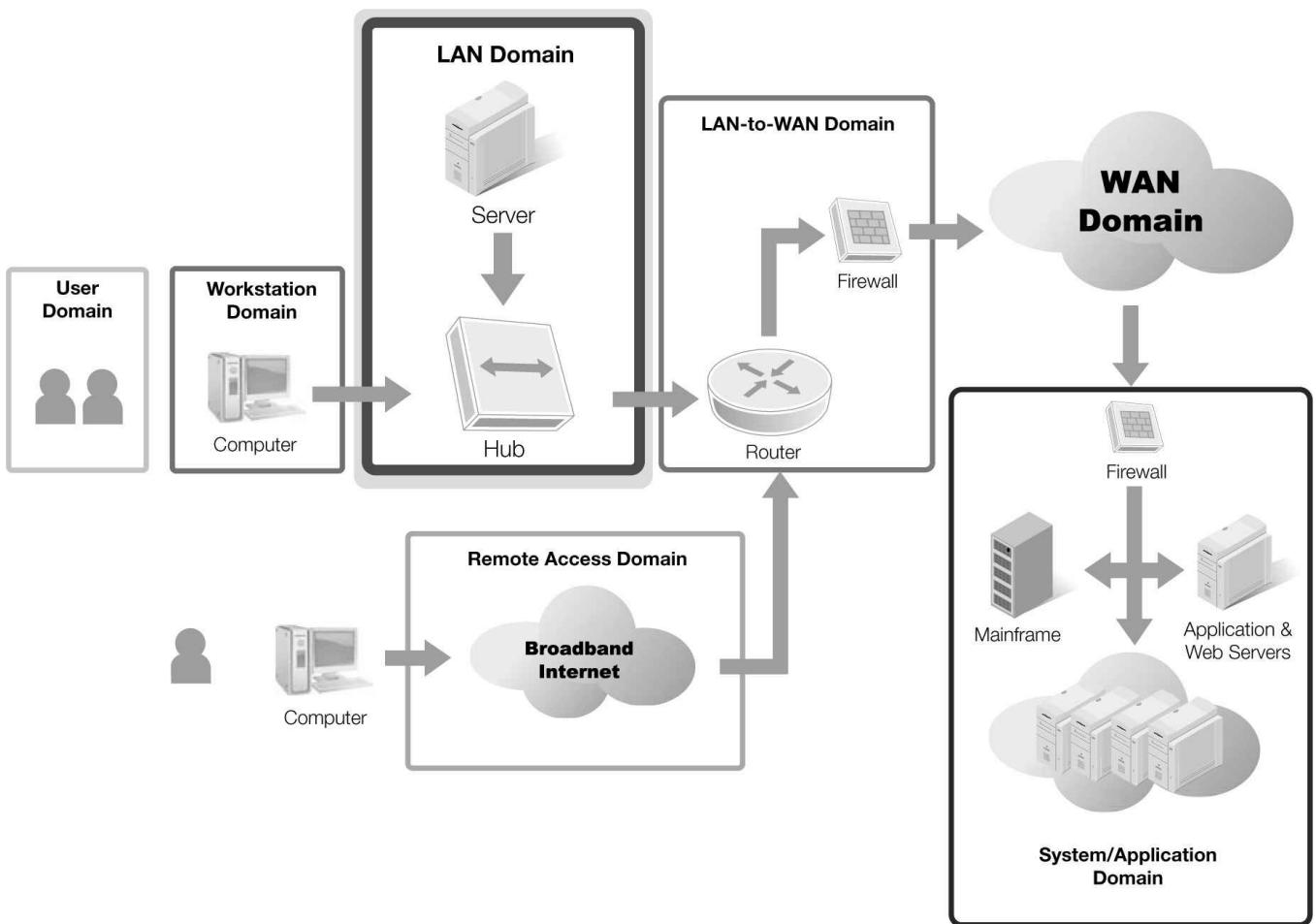


FIGURE 10-1 The LAN Domain within the seven domains of a typical IT infrastructure.

Protecting Data Privacy

When accessing multiple domains, you still must consider the security requirements and control needs for each domain independently of the others. Users still have the responsibility to act in a manner that is acceptable under your organization's security policy, and Workstation Domain controls must still protect local resources. Controls from different domains are distinct but work together to provide a solid defense-in-depth approach to securing your environment.

Now you must consider another domain. Ensuring your organization's private data means designing a layer of controls that protect LAN resources from destruction, alteration, or disclosure by unauthorized users. That means you **must define an authorized user in the context of the LAN Domain**. A user who is authorized to access local resources might not be authorized to access LAN resources on another computer. Compliance with current legislation, regulations, and other requirements means placing appropriate controls in the LAN Domain to ensure all components are secure.

Implementing Proper Security Controls for the LAN Domain

LAN Domain controls often focus on limiting access to remote resources. A **local resource** is any resource attached to a local computer—the same computer to which the user has logged on. A **remote resource** is any resource accessible across the LAN. Of course, the user's computer and the remote resource have to be connected to a network to provide access to the remote resource.

The security controls you'll find in the LAN Domain are similar to controls you'll find in

other domains. The main types of security controls in the LAN Domain include the following:

- Access controls for protected resources, such as printers and shared folders
- Communication controls to limit the spread of malicious software
- Anti-malware software on all computers in the LAN Domain to detect and eradicate malware
- Recovery plans, including backups, for all computers and devices in the LAN Domain
- Procedures to control configuration changes
- Monitoring tools and other detective controls to help detect suspicious LAN Domain activity
- Software patch management for all computers and devices in the LAN Domain

Good LAN Domain security controls will directly support one or more of the three pillars of security in the C-I-A triad, while not interfering with your organization's business functions. A secure system that doesn't support your organization's critical business functions isn't of much use. You will always have to balance security with functionality. Search for compensating controls as often as possible to identify the best controls for both security and functionality. Avoid controls that do not balance these two crucial needs.

Good Control, Bad Control

Suppose you have an expensive color printer connected to your LAN. The printing costs are far more than the amount budgeted because employees use the printer for personal use. One way to solve this problem is to restrict access to the printer to only a few individuals. This approach would solve the printing cost issue but would not allow most users to use the printer for valid business purposes. In this case, the security control gets in the way of regular business functions.

Another way to address the problem is to limit which applications can generate output for the color printer. You could also log all print jobs and audit the printer activity frequently to ensure your users are only submitting valid print jobs. Conducting user training for color-printer use would make these controls (in the User Domain) more effective. These controls working together will be more effective by achieving the original goal without affecting proper business use of the printer.

Devices and Components Commonly Found in the LAN Domain

The LAN Domain's primary responsibility is to provide your users with the ability to connect to and share resources. To meet this goal, the LAN Domain contains four main types of components. These components work together to allow users to share resources on the network and reduce the need for multiple dedicated resources, such as printers, file storage systems, and backup devices. The four main types of components in the LAN Domain are as follows:

- **Connection media**—This includes the adapters and wires (sometimes) that connect components together in the LAN Domain. Not all connection methods use wires. Wireless devices use radio waves to transmit data instead of wires. So, connection media includes wireless adapters.
- **Networking devices**—This includes the hardware devices, such as hubs, switches, and routers, that connect other devices and computers using connection media.
- **Server computers and services devices**—This includes the hardware that provides one or more services to users, such as server computers, printers, and network storage

devices.

- **Networking services software**—This includes the software that provides connection and communication services for users and devices.

Many physical devices in the LAN Domain are actually combinations of several types of components. These components should work together to provide easy access to desired resources and still maintain the security of your organization's information. [Figure 10-2](#) shows common components you'll find in the LAN Domain.

Connection Media

The purpose of any network is to allow multiple computers or devices to communicate with each other. By definition, networked computers and devices are connected to one another and have the appropriate software to communicate. In the past, networked computers and devices were connected using some type of cable. Many of today's networks contain a mix of cables and wireless connections. The cables or devices you use to connect computers and devices to form a network are collectively called **connection media**.



FIGURE 10-2 Common components in the LAN Domain.

Although the technical details of network connections are beyond the scope of this discussion, it is important to have a general understanding of a network's components.

Wired LAN Connections

There are four basic cabling options for physical network connections. Each option has its own advantages and disadvantages. If you choose to use physical cables for part or all of your network, you will have to run cables to each device. Running cables between devices takes careful planning to do it right. Make sure when you explore cabling options that you evaluate the cost of installing all the cables and connection hardware to support both your current and future needs. [Table 10-1](#) lists the four basic cable options, along with the advantages and disadvantages of each one.

TABLE 10-1 Basic network cabling options.

CABLE TYPE	DESCRIPTION	ADVANTAGES AND DISADVANTAGES
Unshielded twisted pair (UTP)	This is the most common type of network cable. UTP generally consists of two or four pairs of wires. Pairs of wires are twisted around each other to reduce interference with other pairs. The most common type of UTP is Category 5 UTP, which supports 100 megabits per second (Mbps) for two pairs of wires and 1,000 Mbps for four pairs.	<ul style="list-style-type: none">• Lowest cost• Easy to install• Susceptible to interference• Limited transmission speeds and distances
Shielded	This is the same as UTP, but with foil shielding around each pair and	<ul style="list-style-type: none">• Low cost

twisted pair (STP)	optionally around the entire wire group to protect the cable from external radio and electrical interference.	<ul style="list-style-type: none"> • Easy to install • More resistant to interference than UTP • Same speed limitations but supports longer run lengths
Coaxial	This is a single copper conductor surrounded by a plastic sheath, then a braided copper shield, and then the external insulation.	<ul style="list-style-type: none"> • Higher cost • Difficult to install • Very resistant to interference • Higher speeds and longer run lengths
Fiber optic	This is a glass core surrounded by several layers of protective materials.	<ul style="list-style-type: none"> • Highest cost • Easy to run cable, although installing end connectors requires special tools • Immune to radio and electrical interference • Extremely high speeds and long run lengths

Communication Protocol

A communication protocol isn't as complex as the name implies. The technical details of each protocol can be quite complex but the concept is simple. A protocol is just a set of rules that parties use to communicate. You use protocol rules every day. For example, suppose you want to invite a person to attend a meeting. If that person is a close friend, you would use an informal greeting and style of conversation. If, on the other hand, the person is an elected official, you would likely use a far more formal greeting and conversation style. You decide how to communicate based on your own protocol rules.

Wireless LAN Connections

Wireless connections are very popular in today's LAN environments, where flexibility is an important design factor. Wireless connections allow devices to connect to your LAN without having to physically connect to a cable. This flexibility makes it easy to connect computers or other devices when running cables is either difficult or not practical for temporary connections. The **Institute of Electrical and Electronics Engineers (IEEE)** defines standards for many aspects of computing and communications. **IEEE 802.11** is a standard that defines **wireless local area network (WLAN)** communication protocols. (A WLAN is a wireless network that covers a small physical area, such as an office or building.) A **protocol** is a set of rules that governs communication.

There are five main protocols in the 802.11 standard. As with the discussion of wired

LAN connections, the technical details are beyond the scope of this discussion, but it is important to know the basic differences among wireless protocols. [Table 10-2](#) lists the five most common wireless LAN protocols.

TABLE 10-2 Common 802.11 wireless LAN standards.

PROTOCOL	MAXIMUM TRANSMISSION SPEED	FREQUENCY*
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	150+ Mbps	2.4 GHz/5 GHz
802.11ac	866+ Mbps	5 GHz

Generally, hardware that supports protocols with faster speeds and a higher range cost more than slower protocols with less range. Your choice of wireless LAN protocol will likely be based on cost, transmission speed requirements, and other devices that might cause interference in a specific frequency.

WARNING

Regardless of the protocol you choose, wireless connections increase the likelihood that unauthorized users will connect to your network. If you choose to implement wireless connections, you must ensure you are using strong access controls and strong wireless encryption.

Networking Devices

After you decide on the types of connections you'll use for your network, you must decide how your components will connect to one another. Few networks have every component connected to every other component. That would make managing your network connections extremely difficult. LANs in today's environments use several types of **networking devices**—hardware devices that connect other devices and computers using connection media—to help keep connections manageable. You'll see many different types of networking devices, but the following three sections discuss the ones you'll commonly use in the LAN Domain.

Hub

The simplest network device is a **hub**. A hub is a box with several connectors, or ports, that allows multiple network cables to attach to it. Common hubs have 4, 8, 16, or even 32 ports. A hub is basically a hardware repeater. A hub takes input from any port and repeats the transmission, sending it as output on every port, including the original input port. A hub makes it easy to connect many devices to a network; you simply connect each device to the hub. [Figure 10-3](#) shows a simple network created using a single hub.

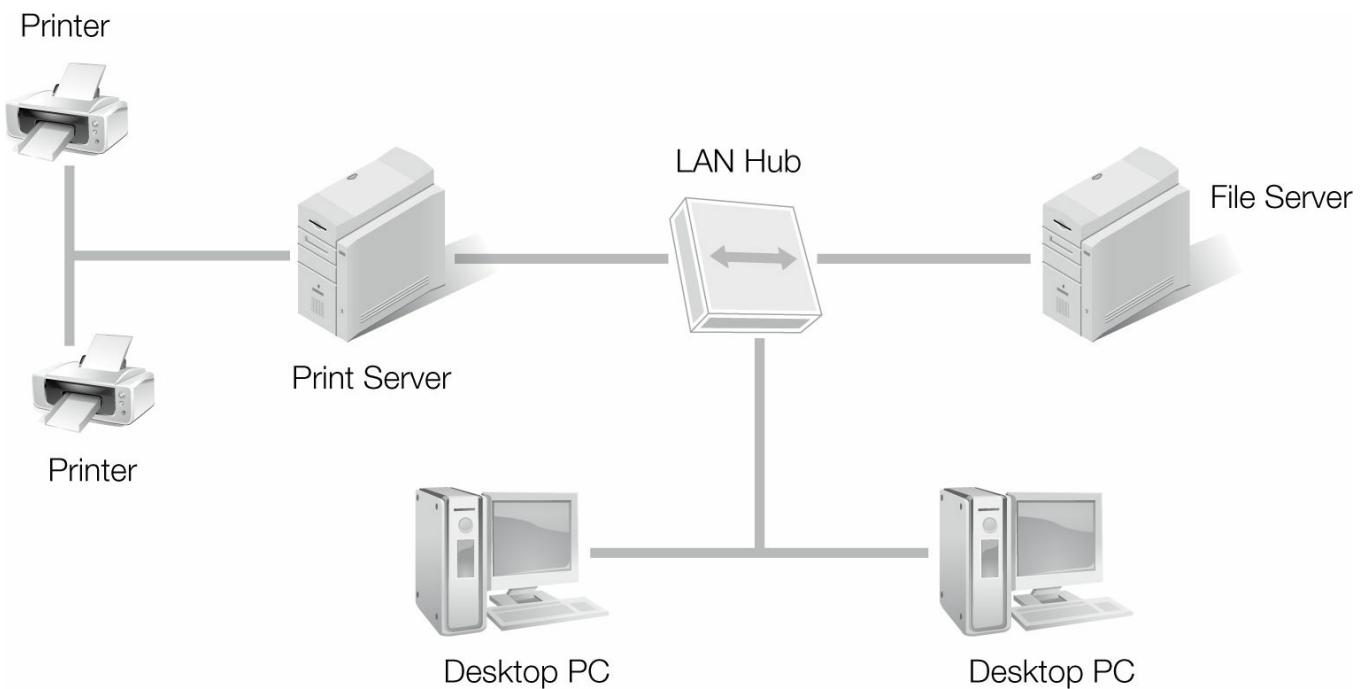


FIGURE 10-3 Simple LAN with a single hub.

Switch

Hubs are very inexpensive devices you can use to connect many computers and devices to a LAN. One problem with hubs is that they repeat all network traffic to all ports. This can cause message collisions and a frequent need to resend messages. Hubs also tend to contribute to network congestion because everyone gets all network traffic. Networks are designed to handle collisions and congestion, but at the cost of slowing down the network. A **switch** can help avoid many collision and congestion issues and actually speed up networks. A switch is a hardware device that forwards input it receives only to the appropriate output port.

For example, if computer A wants to send a message to computer B, a switch will only send the message from computer A to the port to which computer B is attached. No other computers ever see the message. As an additional benefit, if computer C wants to send a message to computer F at the same time computers A and B are talking, the switch can handle both connections without causing a collision. The only computers that actually see information exchanged over the network are the computers involved in the transfer. This is more secure than a hub that repeats messages to all connected computers.

Router

A **router** is another network device that connects two or more separate networks. A router can connect a LAN to another LAN or to devices in another domain in the IT infrastructure. Routers are more intelligent than switches and actually inspect the address portion of the packets on your network. The router examines the destination address and then forwards the packet to the correct outbound port. Routers can be standalone hardware devices or computers with multiple network interfaces running routing software.

Routers also provide an important security capability. You can define rules for each router that tell the router how to filter network traffic. You can restrict which packets you allow to flow through your networks. Routers give you the ability to aggressively control how users and applications use your LANs.

Server Computers and Services Devices

LANs provide easy access to shared resources and shared services. Shared centralized services make it possible for multiple users to share information and physical resources at a lower cost than duplicating information or purchasing devices for every workstation. Shared resources can include both server computers and services devices. Both offer value to a group rather than as a dedicated resource. Examples of shared resources include the following:

- Shared file storage
- Shared printer and print services
- Central database and document management systems

LAN File Server

One common service present even in the earliest LANs is the file-sharing service. A file server is a computer or hardware device that has at least three distinct components:

- One or more connected hard disk drives
- A network interface
- Software to provide network access to files and folders on the attached disks

In the past, most file servers were computers that managed shared folders or file systems. The file server would manage connections and support authorized read/write access to its disks by remote users. Computer-based file servers are still in widespread use, but standalone hardware devices with internal hard disk drives are becoming more popular. Regardless of whether you choose to use a computer or standalone device, a file server's main purpose is to provide secure access to its disk drives for remote users.

LAN Print Server

A print server provides the interface between the LAN and one or more printers. Like file servers, the actual server can be a computer or a standalone hardware device. In either case, the print server accepts print jobs from authorized users and processes them. That means the print server may contain the intelligence to store multiple print jobs and provide advanced abilities to manage the printing process. Print servers vary widely in capabilities but all generally exist to allow multiple remote users to share printers.

LAN Data Storage

LAN data storage might sound like the service the file server provides, but the two services are distinct. A file server just stores files. A data storage server organizes data and attempts to make it more accessible. Data storage software includes database management systems and document management systems. Both types of software provide efficient, effective centralized access to data and documents for remote users.

Another substantial difference you'll notice between file servers and data storage products is that data storage products generally provide far greater control over access authorization. File servers can control access to individual folders and files, but data storage software can control access to the contents of files. Database management systems and document management systems often provide their own features to maintain and authorize users and requests. These systems manage large amounts of data and can grant or deny access to individual pieces of information stored inside very large files. The advantage of data management systems is they can provide fast and efficient access to large amounts of data while maintaining the security of the data down to a very specific level.

Networking Services Software

The last category of components in the LAN Domain is **networking services software**. This category consists of components that really aren't connection or hardware components. All the network computers and components don't do anything without the network software to provide the ability to communicate. The networking services software changes a group of connected devices into a network of devices that communicate to accomplish tasks.

A **network operating system (NOS)** provides the interface between the hardware and the Application Layer software. The NOS provides many of the same functions an operating system provides on a standalone computer. In fact, the roles of the operating system and NOS are so similar that nearly all of today's operating systems contain NOS functionality. Today's networking components generally run either a version of Windows or UNIX/Linux operating systems.

NOS products provide extensive support for resource access and management as well as credential management at various levels. NOSs support low-level authorization as well as higher-level standards such as Kerberos and Active Directory. Choose the NOS that fits best with your existing IT infrastructure.

NOTE

Novell was a leader in early NOS products and many early LANs ran Novell NetWare as their NOS. Today's Novell NOS product is Open Enterprise Server and is based on the SUSE distribution of Linux.

LAN Traffic and Performance Monitoring and Analysis

After you start using a LAN to share resources, how do you know if you are upholding your security policy? You'll learn how to use preventive controls later in this chapter, but you should also use detective controls to validate how your users are using your LAN. Traffic and performance monitoring utilities allow you to watch the traffic flowing across your network. You can watch the traffic in real time or collect it in log files for later analysis.

FYI

Monitoring any resource requires system resources. You will affect your network's performance any time you collect traffic to analyze. Also, you must save a copy of network messages you plan to analyze at a later time. Because networks transport potentially high volumes of information, your saved network messages can require large amounts of disk space to store. It is generally a bad idea to save all network traffic. You should save complete copies of network traffic only when you are investigating a problem and need the extended detail for your analysis.

technical TIP

If you're interested in getting more technical information on packet sniffers and packet analyzers, you can find a list of popular tools at <http://sectools.org/sniffers.html>.

There are two common types of monitoring tools available for monitoring LANs: packet sniffers and network software log files. A **packet sniffer** is software that copies specified packets from a network interface to an output device—generally a file. A sniffer may copy all packets or may select certain packets based on a specific filter, such as source, destination, or protocol. Because sniffers copy the actual packets from the network, you get to see all of the addressing and routing information as well as the contents of each message. If the message is encrypted, you won't be able to read the contents but you will see the encrypted data.

The other common option is to change settings in network software to create audit logging entries for certain packets. You can change configuration settings to log all traffic or just certain conditions. You should only log information you must record to avoid slowing down your network.

After you have a collection of packets, you can use packet analysis software to make sifting through the sniffer output or log files easier. Most analysis software allows you to sort and query data according to your own requirements. You can analyze packets originating from a specific computer or destined for a specific port, or you can analyze queries based on any of the packet's attributes. Using monitoring and analysis tools helps verify appropriate LAN use and identify inappropriate LAN use.

LAN Configuration and Change Management

Suppose you find inappropriate network packets during your LAN traffic analysis. For example, say your traffic analysis revealed a collection of packets originating from an Internet Protocol address that is not valid for your network. In most cases, LAN controls should only allow traffic originating from and addressed to valid addresses. If you initially set up your LAN controls to properly filter network addresses, something is wrong.

One of the first things you should check is the current settings of your routing rules. You should be able to tell if you have defined your routing rules properly. If you find that the rules have changed, determine when the rules changed, who changed them, and why were they changed.

One attack method is to access network devices and change packet filter rules to permit malicious traffic. Another important control in the LAN Domain is network device configuration control and change management. You should implement a formal process to change network configuration settings. A change control board should approve each change. In addition, you should allow only a small number of privileged users to access network devices with the authority to change settings. You should also define your network devices to create audit log entries any time you change a configuration setting. A formal change procedure and configuration change audit will limit unexpected changes to your network configuration and provide an audit trail when changes allow unwanted network traffic.

LAN Management, Tools, and Systems

Managing a LAN means ensuring it fulfills the goals for which it was designed. It also means continually updating the LAN's configuration to satisfy new and updated goals. LAN management covers several related activities, including the following:

- Monitoring LAN performance
- Changing configuration settings to optimize performance

- Changing configuration settings to support new requirements
- Adding necessary controls to address security issues
- Maintaining components of a current recovery process
- Adding, changing, and removing hardware components as requirements dictate
- Mapping LAN components

Although it is possible to manually keep up with the documentation and activities that accompany monitoring and changing your LAN, automated tools can greatly simplify your tasks. In fact, many open source and commercial software packages provide network monitoring and network management functionality. Many networks even have dedicated computers on the LAN running network management software. These dedicated servers are often called **network monitoring platforms (NMPs)**. Because NMP software runs on dedicated servers, it can help manage a LAN by providing monitoring and configuration assistance without having a negative performance impact on other LAN computers and devices. Explore options for network monitoring and management software for your operating system. Software that assists your network administrators will likely simplify the management of your LAN and make it easier to validate compliance with your stated security goals.

technical TIP

For more information on network monitoring and management software, visit these sites:

- Stanford Linear Accelerator Center network monitoring tools,
<http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html>
- SolarWinds free network management tools,
<http://www.solarwinds.com/downloads/#nmCategoryFreeTool>

FYI

Recall the way in which many organizations implement object access controls:

- **Discretionary access control (DAC)**—This defines access permissions based on roles or groups. Object owners and administrators can grant access rights at their discretion.
- **Mandatory access control (MAC)**—This defines access permissions based on data classification and user clearance. Access control is based on object and subject attributes and not on anyone's discretion.

Access Rights and Access Controls in the LAN Domain

LAN access controls limit which subjects can access LAN-based objects. There are generally two levels of controls: computers or devices and users. The first level of control ensures only authorized computers or devices can establish a connection with a target computer or device. The second level of control ensures only authorized subjects can access protected objects.

In the context of networks, any computer or device that is connected to the network is called a **node**. Switches and LAN routers are common places for the first layer of controls. Because these devices establish the network connection between a source node and a target

node, this is a good place to make authorization decisions. Most LAN access controls for nodes compare the identification credentials with stored authentication information.

Identification credentials for nodes can include the interface's **Media Access Control (MAC) address**, Internet Protocol (IP) address, or even a digital certificate. The idea is to select a method to uniquely identify a specific node.

The software running on your switch or router will examine connection requests and compare identification credentials with its own stored credentials to make an authorization decision. A simple way to identify nodes is to use the MAC and IP address the same way user authentication uses an ID and a password. Although not rock solid, it does help identify unauthorized nodes. If your organization requires stronger node identification and authentication, you can use digital certificates. **Digital certificates**, electronic proofs of identity issued by a certificate authority, require more administrative work but provide greater security.

After your LAN establishes a connection between nodes, the second layer of access controls makes an authorization decision for the target object access request. In other words, just because computer A can connect to computer F doesn't mean that all users on computer A are authorized to access files in any shared folder on computer F. At this point, access controls look very much like object-level access controls in other domains. Your node's operating system grants or denies access to objects according to your organization's access control method. In most cases, organizations use either DAC or MAC to define access controls.

technical TIP

You can find an example of switch-level network access control software in the open source product FreeNAC. For more information on FreeNAC, go to
<http://www.freenac.net/en/solutions/lanaccesscontrol>.

At the object level, operating systems grant access based on the requestor's identity. When moving from a single, standalone computer to a network, the concept of user ID becomes a little less concrete. To authorize an access request, the target operating system needs a user ID. There are two main methods you can use to satisfy this requirement:

- Provide identification and authentication with every resource request.
- Provide a secure identification object with every request.

The first approach is simpler but requires that the target environment authenticate the user for each request. This also means you have the problem of whether to replicate all authentication credentials to each target node or to develop a central authentication method. The second approach depends on a central authentication method. Each target node just validates the identification object and proceeds with the authorization process. Common central authentication methods include **Kerberos**, popular in UNIX/Linux environments, and Active Directory domain accounts, which use Kerberos by default. Both options allow a user to sign in only once and use the same credentials for all network resource requests.

From a compliance perspective, it is important to control node connections and object permissions by user or group. You should monitor connections and access for any unusual activity and watch for excessive failures in either connection requests or access requests. Carefully design LAN access controls and monitor for both exceptions and any changes to

your controls' rules. Either type of unusual activity could indicate that an attacker is trying to perform unauthorized actions.

Maximizing C-I-A

One common goal in all domains is the pursuit of the most secure environment possible. Because maximizing the confidentiality, integrity, and availability of your organization's information leads to a secure environment, all of your activities should be to maximize C-I-A.

Maximizing Confidentiality

Ensuring confidentiality in the LAN Domain is one of the simpler tasks. There are basically four steps to ensuring only authorized users can see confidential data:

1. Identify confidential data.
2. Require positive identification for all access requests and define strict access controls for all confidential data identified in Step 1.
3. Use encryption to store all confidential data identified in Step 1.
4. Use encryption to transfer all confidential data identified in Step 1.

You should already be enforcing identification and access controls in the LAN Domain. The new controls involve using encryption. **Encryption** is the process of scrambling data in such a way that it is unreadable by unauthorized users but can be unscrambled by authorized users to be readable again. Specifically, encryption takes **cleartext** data and turns it into **ciphertext** through the use of an algorithm and a key. Cleartext data is simply human-readable data. Ciphertext is the resulting unreadable output.

Encrypting stored data is easy. Today's operating systems support encryption either directly or through integrated software. You can encrypt individual files, folders, volumes, or entire disk drives. After you decide how much data you want to encrypt, explore the various encryption options available for your operating system.

Transmission encryption means never sending information across the network in cleartext, otherwise known as being in the clear. The term *in the clear* means in a format anyone can read during transmission. You can use encryption at the application level or by only allowing encrypted connections between source and destination nodes. Many database management systems and document management systems can also refuse to transmit confidential data over unencrypted connections. Regardless of how you implement encryption, you should validate your controls to enforce encryption and use a packet analyzer to verify that your traffic is actually encrypted.

Maximizing Integrity

LAN nodes are just as susceptible to malicious software as any other computers. As LAN nodes become more powerful and based more on standard operating systems, they become more attractive targets. A compromised LAN node can be just a starting point. Once an attacker gets a foothold in your network, it becomes far easier to compromise other parts of your infrastructure.

You should use the malicious code policies and procedures from the Workstation Domain in the LAN Domain as well. The issues are the same. Ensure you have anti-malware software installed on every computer in the LAN Domain. Establish procedures to ensure all anti-malware software and data are kept up to date. Because some components in the LAN

Domain are devices and not general-purpose computers, you should explore anti-malware features on each device and enable any available features. Your goal is to prevent malicious software from entering your LAN Domain.



WARNING

Don't forget that malware can enter your LAN Domain in other ways. Computers and devices in the LAN Domain often have USB ports, CD/DVD drives, and other ports an attacker can use to introduce malware. Just as in the Workstation Domain, ensure you control access to external media. Don't allow external media except when you absolutely need it.

Malware is not the only integrity concern. Users can also violate data integrity. Users can be malicious or unaware of their actions. Either way, it is important to control changes to critical data. Good access controls should stop any data changes by unauthorized users. You can also audit changes to critical data by authorized users. Audit data can provide valuable audit trails for later analysis. Good audit trails can help trace unauthorized changes back to their source. Getting to the root of unauthorized changes should provide the input needed to modify or add controls to keep the damage from happening again.

Maximizing Availability

It is important to develop and maintain a comprehensive recovery plan to replace lost or damaged data. As you use LANs to store more information in central repositories, it becomes more important to ensure the data is available when users request it. A crucial part of your security plan is creating secondary copies, or backups, of your data in case the primary copy is damaged or deleted. Because more users are sharing the same set of data, any loss affects a larger portion of your organization.

A solid recovery plan contains a schedule for creating backups as well as the procedures for recovering lost or damaged data. All current NOS products include capable utilities to back up and recover data. Third-party vendors also provide solutions that make enterprise-wide backups easier than managing individual computers. Explore the backup solutions available for your choice of server computers and select the one that meets your security needs with minimal administrative oversight.

Most backup and recovery solutions target networked computers. Don't forget to include any network devices with valuable data in your backup and recovery plan. Some network devices store configuration settings and performance data. Backing up these devices can save valuable log and performance data and make reconfiguring a device after a failure much faster. In nearly all cases, it is faster to load backed-up configuration data than to re-enter it manually. Make sure your backup plan includes any devices with data you'll need if a device fails.

Another important aspect of availability is ensuring your users can access LAN resources in an acceptable time frame. If the network is too slow, users can't get to their requested information and you are not supporting data availability. In some cases, this problem is just due to excessive network use or a lack of network capacity for normal use. In both cases, you must examine the behavior and reduce the load on your network, increase its capacity, or both.

In other cases, a lack of availability results from an attack. Suppose your organization sells automobile insurance. You attract new customers by offering to analyze their existing coverage and providing a competitive quote showing how your coverage saves them money.

You depend on your database of coverage costs to generate the analysis report. You cannot conduct business if you cannot access your database. In this case, an attacker that renders your network unusable effectively stops your ability to conduct business. The type of attack that denies access to a critical resource or service is called a **denial of service (DoS)** attack.

The best defense against DoS attacks is to aggressively enforce access controls and monitor your network for unusual or excessive traffic. You'll need to provide evidence that you've implemented both preventive and detective controls to combat DoS attacks.

Managing the Vulnerability of LAN Components

Attackers never stop exploring new ways to compromise information systems. You must constantly make efforts to stay ahead of the attackers. As soon as new attacks surface, most hardware and software developers make changes to their products to address the new attacks. Nearly every hardware and software vendor releases updates to address vulnerabilities in their products. You should establish procedures to ensure all components in the LAN Domain are up to date.

Operating System Patch Management

Because operating systems play such a crucial role in granting or denying access to resources, they are a prized target for attackers. If an attacker can compromise the operating system, many attacks are possible. To keep your operating system as secure as possible, you should acquire and install all security-related patches, updates, and service packs. All current operating systems provide methods for automatically identifying, downloading, and installing updates. Either use your operating system's capability for automatic updates or develop procedures to keep your operating systems as current as possible.

Application Software Patch Management

Applications are also prime targets for attackers. Database management systems and document management systems commonly control access to critical data through application access controls. Attackers who compromise applications can often bypass these controls and compromise your data. Just as with your operating systems, you should establish procedures to frequently identify any security updates and install those on your applications to keep your LAN Domain as secure as possible.

Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines

Compliance in the LAN Domain depends on implementing the best controls. As with all domains, you can meet some goals using different controls. Don't just accept the common controls. Take the time to explore alternative controls for each security goal. Some controls will have more of an impact on your organization than others. If two controls provide the same assurance but have different levels of impact on your organization, choose the one that has less of an impact.

As you analyze controls in the LAN Domain to meet compliance requirements, ensure each control satisfies your security policy. If a control does not support any part of your security policy, you should question its value to your organization. Although different

legislation, regulations, and vendor standards have different requirements, Table 10-3 lists some types of controls you'll likely need to ensure components in your LAN Domain are compliant.

Implementing multiple types of controls decreases the likelihood an attack will be successful and makes your LAN Domain more secure.

TABLE 10-3 Preventive, detective, and corrective controls in the LAN Domain.

CATEGORY OF CONTROL	TYPE OF CONTROL	DESCRIPTION
Preventive	Node-based access controls for LAN nodes	Only allow authorized nodes to establish connections.
	User-based access controls for LAN resources	Only allow authorized users to access resources.
	Configuration change control	Limit changes to network device configuration settings and filtering rules.
	Encryption	Enforce encryption for stored data and transmitted data for confidential information.
Detective	Connection request auditing	Log connection failures for all connections and successes for high-value targets.
	Object access auditing	Log access failures for most objects and successes for critical objects.
	Performance monitoring	Frequently sample network traffic flow metrics and alert for any unusual activity.
	Packet analysis	Examine packets for known attack signatures and to ensure necessary data is encrypted.
	Configuration settings monitoring	Compare LAN device configuration settings with stored baselines to detect any unauthorized changes.
Corrective	Operating system and application patching	Keep applications and operating systems patched to the latest available level.
	Attack intervention	Automatically modify filtering rules to deny traffic from sources generating known attack signature packets.

Best Practices for LAN Domain Compliance

The LAN Domain for any organization often contains the bulk of an organization's sensitive information. Most organizations want to make their information available to as many users as need it, while still keeping it secure. Protecting information in the LAN Domain focuses on maintaining the balance between easy access and solid security. In reality, solid planning can provide both.

The following best practices represent what many organizations have learned. Plan well and you can enjoy a functional LAN Domain that makes information available for use. Here are general best practices for securing your LAN Domain:

- Map your proposed LAN architecture before installing any hardware. Use one of the several available network-mapping software products to make the process easier. Identify all of the components and connection media you'll need for now and for future growth. Update the network map any time you make changes to your network.
- Implement a single sign-on strategy for your environment to keep users from signing on

multiple times as they use network resources.

- Identify critical resources and establish detailed access controls.
- Develop a backup and recovery plan for each component in the LAN Domain. Include recovery plans for damaged or destroyed connection media. Don't forget to include configuration settings for network devices in your backup and recovery plan.
- Implement frequent update procedures for all operating systems, applications, and network device software and firmware.
- Define routing and filtering rules to only allow necessary traffic in the LAN Domain.
- Monitor LAN traffic for performance and packets for suspicious content.
- Carefully control any configuration setting changes or physical changes to your LAN. Update your network map after any changes.
- Enable connection and object access auditing on items of interest.
- Use automated tools whenever possible to map, configure, monitor, and manage the LAN Domain.
- If your components support active attack intervention, configure devices to terminate connections when a suspected attack is in progress.

As with all best practices, these are only a starting point. Implement the points that are appropriate for your environment. Doing so will get you started toward establishing and maintaining a secure LAN Domain.



CHAPTER SUMMARY

In this chapter, you learned about how important the LAN Domain is to any organization. Because you probably store much of your organization's shared information in the LAN Domain, it is crucial that you secure all components in the domain. You learned about the components commonly found in the LAN Domain and the importance of monitoring and configuring components properly. You learned about some of the most important security controls and how to maximize C-I-A in the LAN Domain.

All of the domains in the IT infrastructure are important. Although it might be difficult to highlight any one domain over the others, the LAN Domain does tend to be where much of an organization's critical data resides. Along with securing other domains, your organization's information security depends on securing the LAN Domain.



KEY CONCEPTS AND TERMS

Ciphertext

Cleartext

Connection media

Denial of service (DoS)

Digital certificates

Encryption

Hub

IEEE 802.11

Institute of Electrical and Electronics Engineers (IEEE)

Kerberos

Local resource

Media Access Control (MAC) address

Network monitoring platforms (NMPs)

Network operating system (NOS)

Networking devices

Networking services software

Node

Packet sniffer

Protocol

Remote resource

Router

Switch

Wireless local area network (WLAN)



CHAPTER 10 ASSESSMENT

- 1.** A LAN is a network that generally spans several city blocks.
 - A. True
 - B. False
- 2.** A local resource is any resource connected to the local LAN.
 - A. True
 - B. False
- 3.** Which of the following devices repeats input received to all ports?
 - A. Switch
 - B. Hub
 - C. Gateway
 - D. Router
- 4.** _____ cabling provides excellent protection from interference but can be expensive.
- 5.** Even the newest wireless protocols are slower than using high-quality physical cable.
 - A. True
 - B. False
- 6.** Which LAN device commonly has the ability to filter packets and deny traffic based on the destination address?
 - A. Router
 - B. Gateway
 - C. Hub
 - D. Switch
- 7.** Which of the following would be the best use for a packet sniffer?
 - A. To approve or deny traffic based on the destination address
 - B. To encrypt confidential data
 - C. To analyze packet contents for known inappropriate traffic
 - D. To track configuration changes to specific LAN devices
- 8.** Why is LAN device configuration control important?

- A. Configuration control helps to detect violations of LAN resource access controls.
 - B. Configuration control can detect changes an attacker might have made to allow harmful traffic in a LAN.
 - C. It reduces the frequency of changes because they are more difficult to implement with configuration control.
 - D. Configuration control ensures LAN devices are set up once and never changed.
- 9.** A(n) _____ is a dedicated computer on a LAN that runs network management software.
- 10.** Which of the following controls would comply with the directive to limit access to payroll data to computers in the HR department?
- A. User-based authorization
 - B. Group-based authorization
 - C. Media Access Control-based authorization
 - D. Smartcard-based authorization
- 11.** You should back up LAN device configuration settings as part of a LAN backup.
- A. True
 - B. False
- 12.** A successful DoS attack violates the _____ property of C-I-A.
- 13.** Where must sensitive information be encrypted to ensure its confidentiality? (Select two.)
- A. While in use on a workstation
 - B. During transmission over the network
 - C. As it is stored on disk
 - D. In memory
- 14.** Why is mapping a LAN a productive exercise?
- A. Visual maps help to identify unnecessary controls.
 - B. Visual maps help in understanding your LAN design.
 - C. A LAN map is required before physically installing any hardware or connection media.
 - D. A visual map is the only way to define paths between devices.
- 15.** How can some smart routers attempt to stop a DoS attack in progress?
- A. They can alert an attack responder.
 - B. They can log all traffic coming from the source of the attack.
 - C. They can terminate any connections with the source of the attack.
 - D. They can reset all connections.

CHAPTER 11

Compliance Within the LAN-to-WAN Domain

T

ODAY'S INFORMATION SYSTEM ENVIRONMENTS depend on distributed architectures. In

the past, clients, application software, and data tended to exist close to one another. As networks grew to be faster and more stable, clients and applications began to move away from centralized data storage. Now, networks are mature enough to support larger and larger spans between different elements that make up an application. It is common to see enterprise applications in which data, clients, and even segmented applications reside in completely different network environments.

The key to supporting such an environment depends on the ability to connect local resources on a local area network (LAN) to resources on another network. The most popular mechanism is the wide area network (WAN). The purpose of the **LAN-to-WAN Domain** is to provide stable and controlled access from LAN resources to a WAN. You must ensure your data is secure in the LAN-to-WAN Domain as well as in all other domains. In this chapter, you'll learn about the LAN-to-WAN Domain and how to ensure compliance in this domain.

Chapter 11 Topics

This chapter covers the following topics and concepts:

- How compliance law requirements relate to business drivers
- Which devices and components are commonly found in the LAN-to-WAN Domain
- What LAN-to-WAN traffic and performance monitoring and analysis are
- What LAN-to-WAN configuration and change management are
- Which LAN-to-WAN management tools and systems are commonly used
- What access rights and access controls in the LAN-to-WAN Domain are
- How to maximize C-I-A
- How to perform penetration testing and validate LAN-to-WAN configuration
- How to ensure adherence to documented IT security policies, standards, procedures, and guidelines
- What best practices for LAN-to-WAN Domain compliance are

Chapter 11 Goals

When you complete this chapter, you will be able to:

- Understand compliance law requirements and business drivers
- Compare how devices and components found in the LAN-to-WAN Domain contribute to compliance

- Describe methods of ensuring compliance in the LAN-to-WAN Domain
- Summarize best practices for LAN-to-WAN Domain compliance

Compliance Law Requirements and Business Drivers

Many of today's applications are deployed as **distributed applications**. A distributed application is one in which the components that make up the application reside on different computers. In many cases, the components reside in different networks. Although the actual applications and resources belong in other domains, you'll need to govern access and data flow to and from your LAN Domain. That is the purpose of the LAN-to-WAN Domain. As distributed applications and remote resources connected using WANs are becoming more and more useful to authorized users and attackers, it is more important than ever to ensure compliance within the LAN-to-WAN Domain. [Figure 11-1](#) shows the LAN-to-WAN Domain in the context of the seven domains in the IT infrastructure.

It's not enough to keep your information secure sometimes. Keeping your information secure means keeping it secure at *all* times. This is especially true as it moves between domains in the IT infrastructure. As organizations rely more and more on remote resources and applications, it becomes crucial to ensure your data is secure as it travels from location to location. A solid security policy that includes compliance with all appropriate requirements should support efficient and cost-effective operation. Implementing the controls necessary to support your security policy in the LAN-to-WAN Domain makes your organization more secure and more effective.

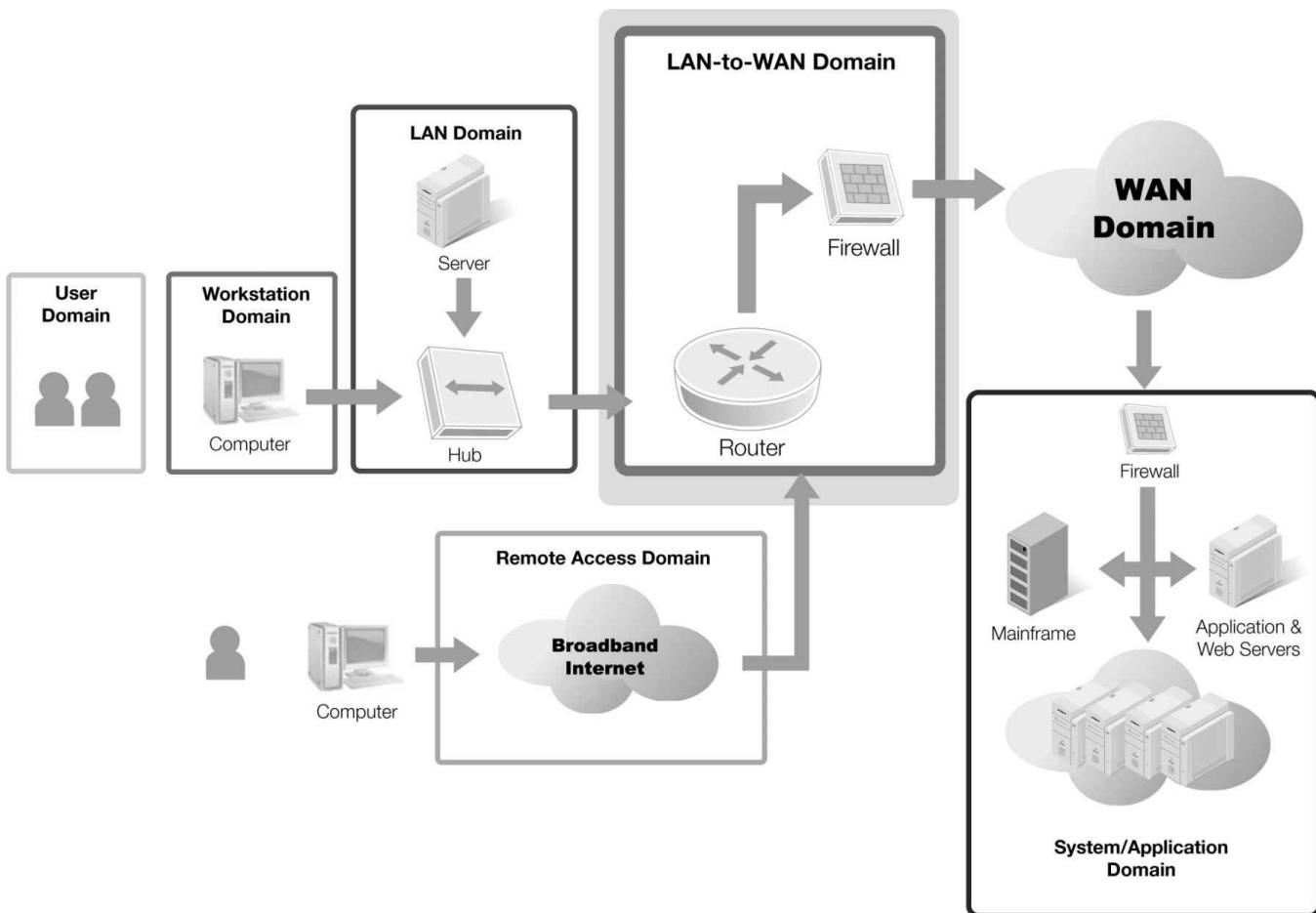


FIGURE 11-1 The LAN-to-WAN Domain within the seven domains of a typical IT infrastructure.

Protecting Data Privacy

Your organization may implement applications you develop or applications developed by someone outside your organization. In either case, parts of the application likely exchange data with other parts of the application to perform intended functions. The current architecture of many distributed applications involves a client sending input data to a remote program, or **service**, and then receiving the results returned from the remote program. A service is a set of software functionality that a client accesses using a prescribed interface. [Figure 11-2](#) shows the exchange of data in a remote service call.

One of the main concerns when sending data across public networks is confidentiality. Although not all data is confidential, any data you exchange with a remote resource using a WAN is potentially available for anyone else to see. Consider all WANs to be hostile and insecure. Your organization likely controls access to your LANs and has some measure of assurance of how private the LANs are. WANs are different. You don't have control over who accesses a WAN or who can access data traveling across it. You must deploy sufficient controls to protect the privacy of any data in the LAN-to-WAN Domain.

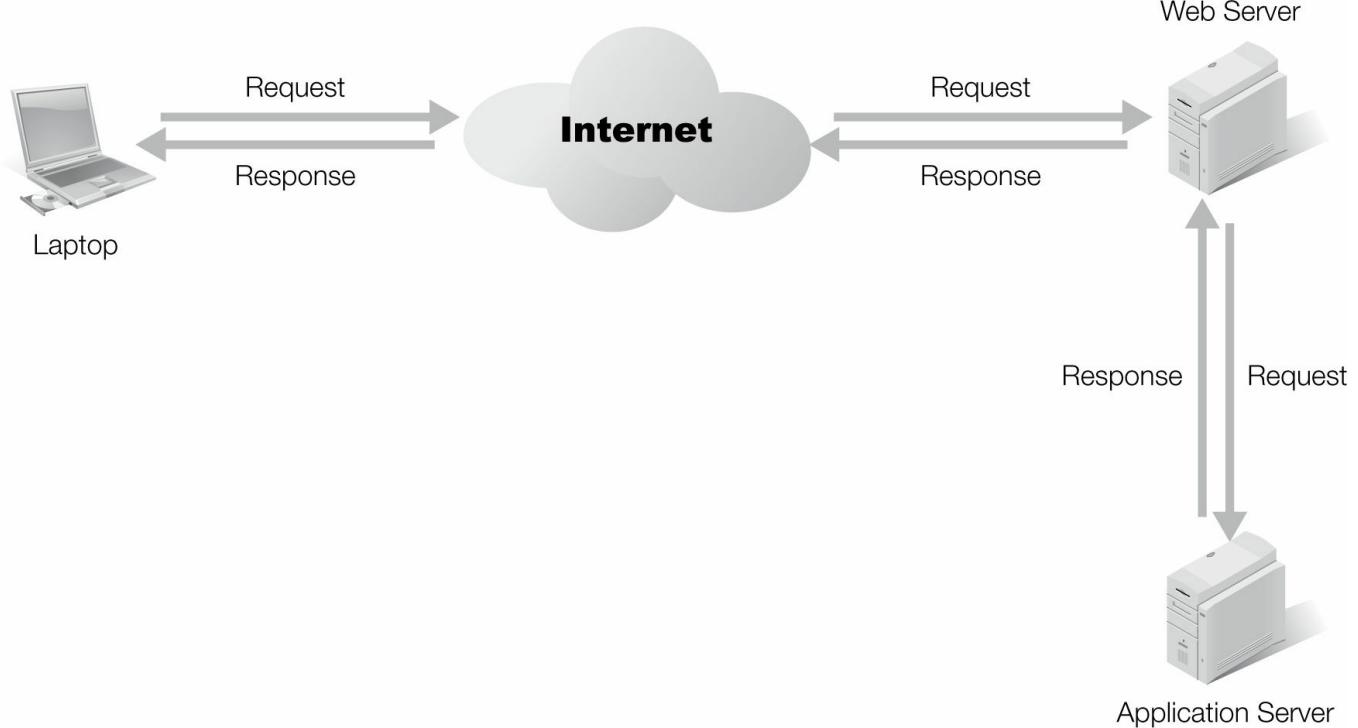


FIGURE 11-2 Exchanging data with a remote service.

Implementing Proper Security Controls for the LAN-to-WAN Domain

The primary control type you'll use in the LAN-to-WAN Domain for any data passing through is traffic filtering. You'll learn that there are different devices and types of filtering, but make sure you aggressively use filtering to stop any inappropriate traffic from flowing in, out, or through your LAN-to-WAN Domain. A collection of well-placed and well-configured firewall devices can dramatically increase your network's ability to withstand attacks.

Another important control anytime data flows in or out of the LAN-to-WAN Domain is encryption. There are many encryption choices, and the right control depends on how you'll use the data and which component applies the encryption method. Your application may encrypt your data in another domain. You'll learn about different approaches later in this chapter. Some solutions require multiple layers of controls. You select the best controls that support a few general principles:

- No data in the LAN-to-WAN Domain should ever be transmitted in cleartext. Anyone can read cleartext data or data that is in the clear.
- When using encryption, select the algorithm based on needs. Don't just select the largest key.
- Assume an attacker can intercept and examine any network messages.

Devices and Components Commonly Found in the LAN-to-WAN Domain

The LAN-to-WAN Domain represents a point of transition between more secure LANs and far less secure WANs. In this section, you'll learn about the devices and components you'll commonly find in the LAN-to-WAN Domain. Once you've learned about the devices and components, you'll learn about controls to ensure compliance in the LAN-to-WAN Domain.

Routers

A router is a network device that connects two or more separate networks. In the context of the LAN-to-WAN Domain, a router makes the actual connection between the LAN and the WAN. A router can be a standalone network device or it can be software that runs on a computer. In either case, the hardware must contain at least two network interfaces—one for each network. A router works by inspecting the address portion of the packet and forwarding the packet to the correct network.

The process of examining each packet is time consuming and can slow your network down. Newer network devices and software often contain support for **Multiprotocol Label Switching (MPLS)**. MPLS networks add a simple label to each network packet. The routing devices in the network forward packets based on the address in the label as opposed to data in the header portion of the packet. MPLS can dramatically increase the speed and usefulness of your network in two important ways:

- MPLS takes less time to process each packet because the router only has to look at the packet's label.
- MPLS devices create virtual links between nodes that can transport higher-level encrypted packets.

▶ NOTE

The term *firewall* refers to the fireproof wall that separates sections of buildings. The purpose of a firewall in construction is to limit the damage a fire can cause. If one section of a building catches fire, the fire will not spread beyond the firewalls and will be contained. Firewalls don't minimize damage to the section of the building that is burning—they just keep the fire from spreading and causing more damage.

Firewalls

A **firewall** is a network security measure designed to filter out undesirable network traffic. Like a router, a firewall can be a network device or software running on a computer. Firewalls provide an important security capability. You can define rules for each firewall that tell the firewall how to filter network traffic. You can restrict which packets you allow to flow through the LAN-to-WAN Domain. Firewalls give you the ability to aggressively control what types of information can travel between your LANs and WANs.

The simplest type of firewall is a packet-filtering firewall. The firewall examines each packet and decides on an action to take after comparing the packet's attributes with the firewall rules. Rules commonly instruct firewalls to deny or forward packets based on the target application, Internet Protocol (IP) address, and port. You can create rules based on other criteria as well. However, protocol, IP address, and port filtering give you the ability to restrict most unwanted traffic from passing through the firewall.

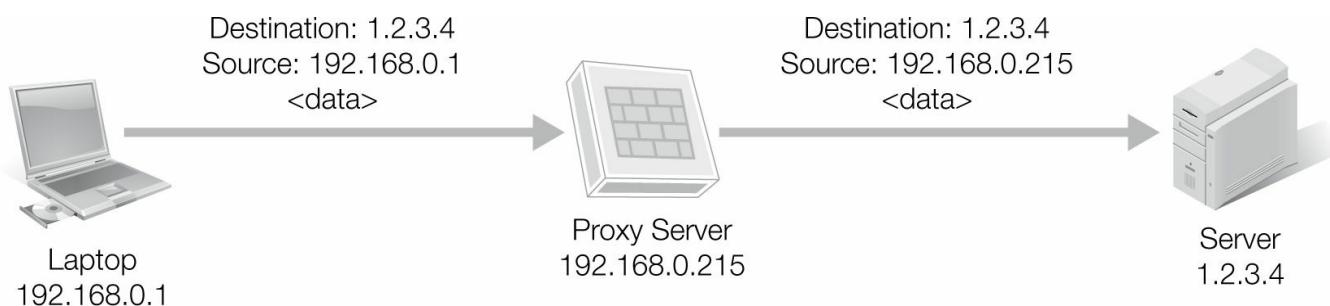


FIGURE 11-3 Network request using a proxy server.

Proxy Servers

A **proxy server** is a type of firewall that makes requests for remote services on behalf of local clients. The proxy server receives a request from a client and evaluates the request based on its defined rules. If it determines that the request is authorized, the proxy server forwards the packets to the remote server, using its own IP address as the source address. In this way, a proxy server hides the true source's identity. The remote server only sees the IP address of the proxy server. [Figure 11-3](#) shows how a proxy server forwards requests to remote resources.

The proxy server keeps a record of sent messages in an internal table. Unless an error occurs, the remote server should send a response to the initial request. When the proxy server receives the response, it looks up the true address of the client that sent the original request and forwards the response to the client.

Proxy servers have several uses. Because they process all network traffic between clients and remote servers, they work well as content filters. Proxy servers can filter unwanted or inappropriate content using many different types of rules. Web content filters examine Web-based traffic and can block Web content that does not adhere to your organization's Internet or Web acceptable use policy (AUP).

Demilitarized Zones

The LAN-to-WAN Domain marks an important transition for data. Data flowing from a WAN to your LAN moves from an unsecure domain to a secure domain. It is generally a poor idea to allow any users to access resources inside your secure LANs. It is important to positively identify users to properly control access to your organization's resources. On the other hand, many organizations do want to provide internal information to anonymous users. For example, most online retailers want anonymous users from the Internet to visit their sites and browse through their products. How do you allow anonymous users to access your data without compromising it?

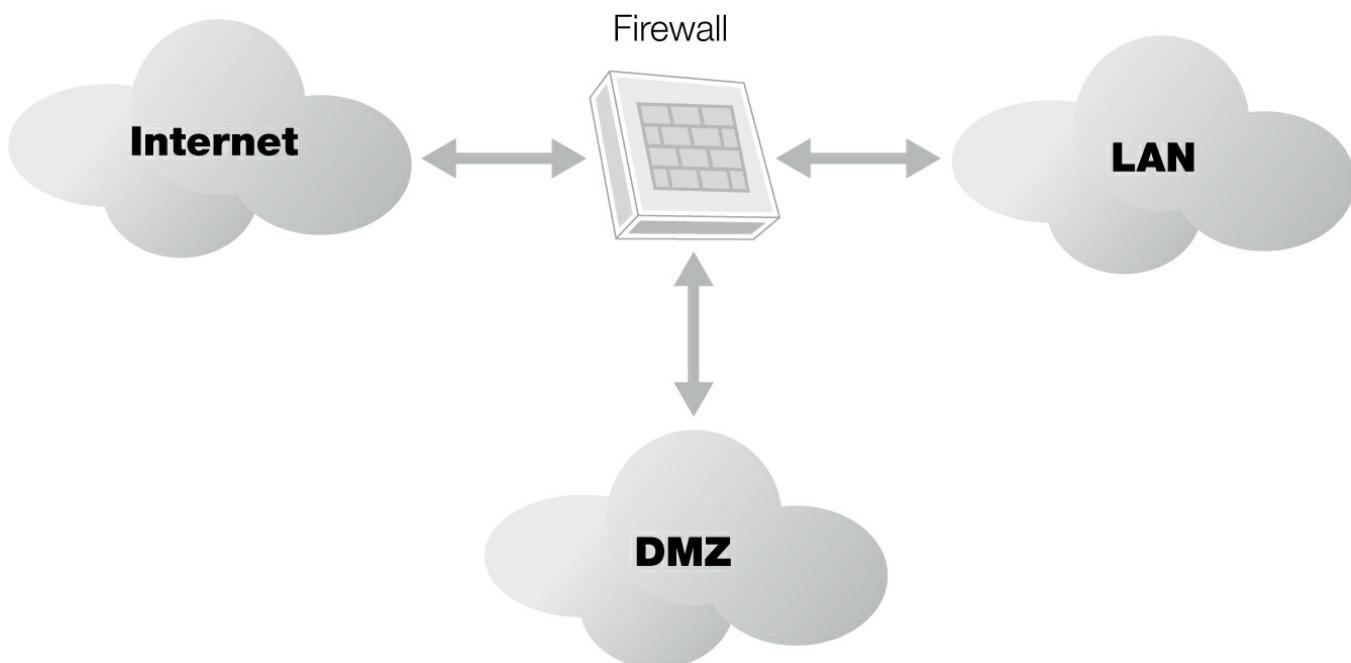


FIGURE 11-4 Simple DMZ with one firewall.

The answer lies in creating an area of your IT infrastructure that allows access for anonymous users but aggressively controls information exchanges with internal resources. This special zone is connected to both the Internet and your internal secure network. The term for this zone is a **demilitarized zone (DMZ)**. A DMZ is a separate network or portion of a network that is connected to a WAN and at least one LAN, with at least one firewall between the DMZ and the LAN. [Figure 11-4](#) shows a simple DMZ with one firewall.

A very common use of DMZs is for Web servers. Users from the Internet can access your Web server and see pages generated from the Web server. The Web server can make limited connections to your application and database servers in your LAN. The firewall blocks connections from Internet users to your LAN but allows the Web server to connect. One danger is that an attacker could compromise your Web server and use it to either connect to your LAN resources or perhaps use the Web server to launch attacks on other computers. To help protect your DMZ servers from launching attacks, you can add a second firewall between the DMZ and the WAN. This firewall would filter outbound traffic and would stop attacks originating from within your DMZ. [Figure 11-5](#) shows a DMZ with two firewalls.

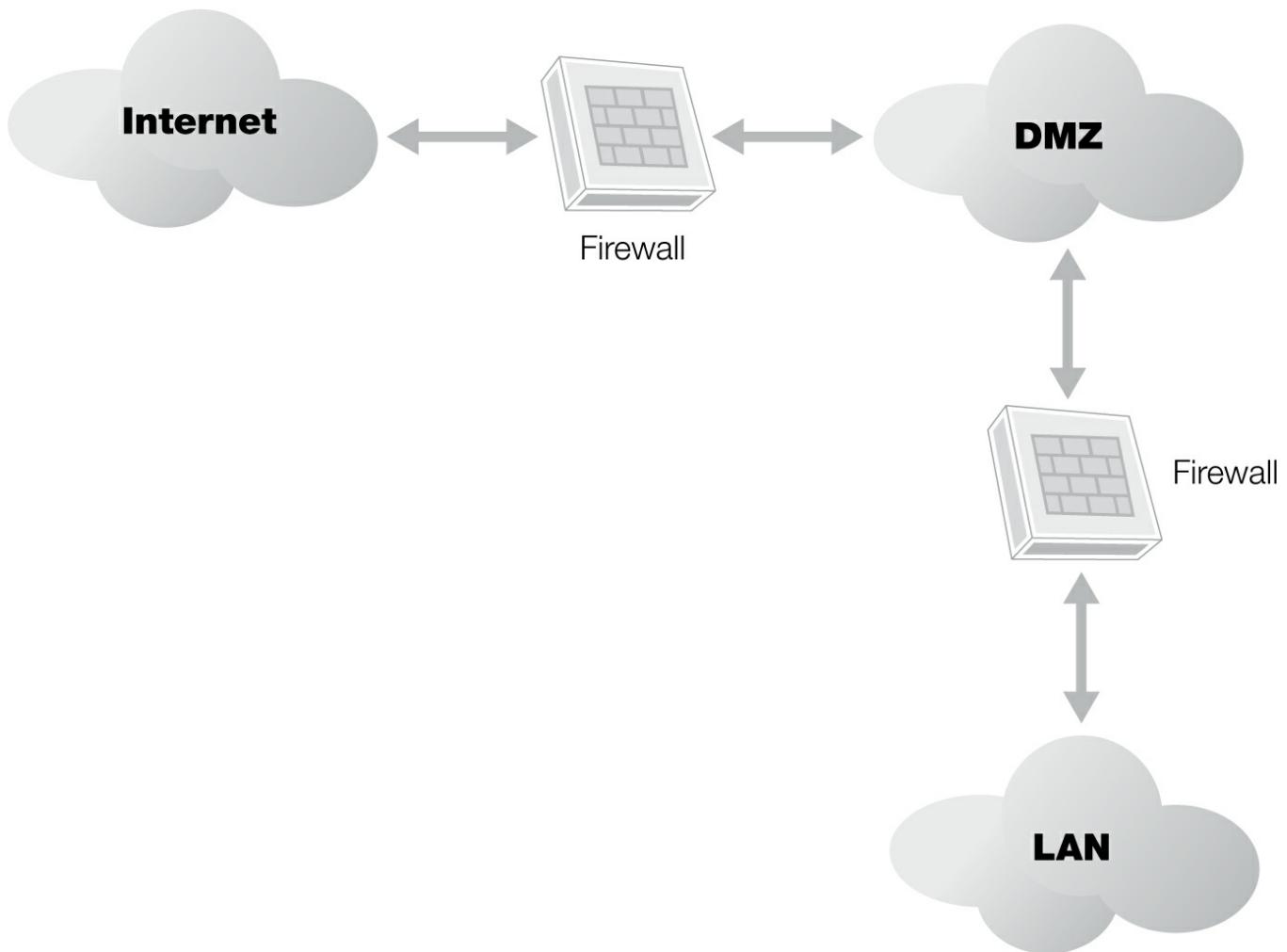


FIGURE 11-5 DMZ with two firewalls.

Honeypots

A **honeypot** is a server deliberately set up to trap attackers. You set up a honeypot with software and data that is configured to be both unsecure and interesting to attackers. The idea of a honeypot is to divert the attention of attackers away from real items of interest. You can configure the software running on the honeypot to alert you when an attacker accesses resources. This gives you the ability to track the attacker's actions and learn more about the techniques being used against legitimate targets. Perhaps you might even track down the attacker's location.

There are at least two dangers with honeypots. First, a honeypot that is connected to your LAN could provide an attacker with an entry point to your LAN. If the attacker successfully compromises the host, the attacker could access protected LAN resources. Second, an attacker with any skill will likely eventually realize the honeypot for what it is. An attacker might assume an organization that goes to the trouble of setting up a honeypot might have a truly valuable resource they are trying to hide. In this case, the honeypot actually draws more attention to your valuable resources instead of diverting attention away.



WARNING

A honeypot is often viewed by attackers as a challenge. Many attackers feel they are being taunted. Given a bruised ego, attackers might execute follow-on attacks to get even for being

tricked.

Honeypots require near-constant attention, both automated and by personnel. When a honeypot goes ignored for too long, the dangers just mentioned become real risks with dire consequences.

Internet Service Provider Connections and Backup Connections

The purpose of the LAN-to-WAN Domain in most organizations is to provide a method to connect your LANs to the Internet. Connecting to the Internet is easier than ever before. All you have to do is establish an account with an **Internet service provider (ISP)**. The ISP provides at least one method to connect your device to its network. After you have connected to its network, the ISP routes traffic from your environment to the Internet.

You can establish service using different connection methods. The most popular methods are as follows:

- Dial-up
- Digital subscriber line (DSL)
- Cable modem
- Wireless
- Dedicated high-speed connection, such as a T3 or SONET

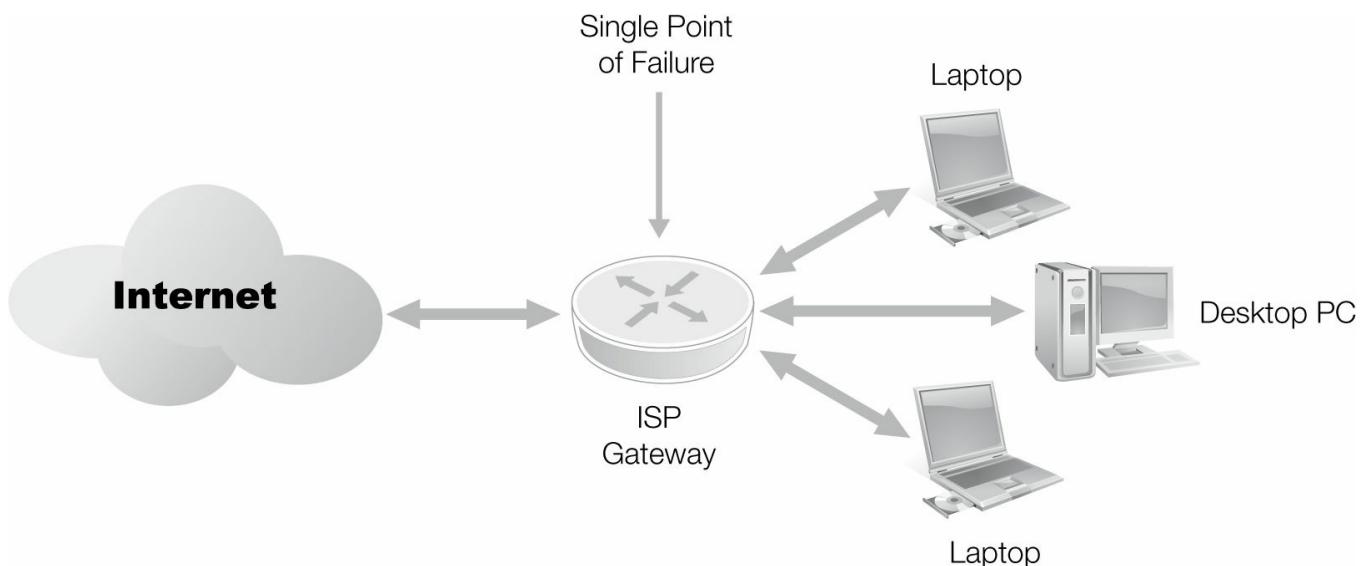


FIGURE 11-6 ISP connection single point of failure.

Regardless of which connection medium you choose, your network relies on the connection to your ISP to establish Internet connections. If the connection to your ISP goes down for any reason, you'll lose your connection to the Internet. A single ISP connection means a **single point of failure**. With a single point of failure, many components depend on a single component. If the single component fails, all other dependent components essentially fail as well. [Figure 11-6](#) shows a single ISP connection that represents a single point of failure.

Make sure you develop an alternative Internet connection plan to avoid a single point of failure. You'll learn how to accomplish this in the "Dual-Homed ISP Connections" section later in the chapter.

Intrusion Detection Systems/Intrusion Prevention Systems

Firewalls are extremely effective at filtering out known unwanted traffic. However, attackers are getting more and more sophisticated all the time. A firewall is only as good as its rules. Because most firewall rules are based on static attributes, they aren't effective at protecting a network from all types of attacks.

For example, suppose an attacker compromises one of your trusted servers and installs a distributed denial of service (DDoS) agent. On command, the agent starts sending large volumes of messages to different hosts. Your firewall sees all the messages but forwards them because they originated from a trusted server. The result is a successful DDoS attack.

A type of network measure that can help in this situation is an **intrusion detection system (IDS)**. An IDS is either a network hardware device or software that monitors real-time network activity. It compares the observed behavior with performance thresholds and trends to identify any unusual activity. If it does identify unusual activity, it sends a notification to someone who can explore the situation and react appropriately. Some systems provide the ability to automatically take action. An **intrusion prevention system (IPS)** extends the IDS capability by doing something to stop the attack. In the preceding example, the IPS could modify firewall rules to deny any traffic originating from the compromised server. This simple action would stop the attack.

Data Loss/Leak Security Appliances

As the volume of information flowing around networks increases, so does the concern that sensitive data will leak out of the protected environment into the public domain. Compliance requirements often place restrictions on data and how you must handle it. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires your organization to protect credit card numbers both at rest and in transit. You can ensure your applications and databases protect credit card numbers, but what about other forms of data transfer? How do you protect credit card numbers in e-mail messages?

Data leak security appliances (also called *data loss security appliances*) are network devices or software running on computers that scan network traffic for data-matching rules. The rules differ for each organization but would likely include patterns for matching credit card numbers, Social Security numbers, and other sensitive information for organizations enforcing PCI DSS compliance. Other requirements for protecting sensitive data would result in additional rules. The data leak security appliance helps detect and prohibit data that would otherwise leak to the public due to oversight or error. It is one more layer in a multilayered approach to security.

Web Content Filtering Devices

As you learned earlier, a Web content filter is a specific type of proxy server. In addition to forwarding Web requests to a remote Web server, the filter scans all traffic and applies content rules. These content rules conform to the organization's Internet AUP. Web content filters are common in many organizations that provide Internet access. The goal is to provide Internet access that is necessary or desired for appropriate users while denying inappropriate Internet use.

A Web content filter evaluates content based on several different criteria, including the following:

- **Blacklist**—This provides a list of uniform resource locators (URLs) or Domain Name

System (DNS) entries from which all transfers are blocked.

- **URL filter**—This involves scanning and evaluating URLs for inappropriate content using a dictionary of inappropriate search items.
- **Content keyword filtering**—This involves evaluating text in content for inappropriate content using a dictionary of inappropriate search terms.
- **Content analysis**—This involves evaluating text and non-text content for inappropriate content.

Traffic-Monitoring Devices

Traffic-monitoring devices monitor network traffic and compare performance with a baseline. Traffic monitors can help detect network issues by identifying performance problems and alerting administrators of the problem. Network problems can be caused by the following:

- Denial of service (DoS) or DDoS attacks
- Device or communications failure
- Bandwidth saturation

In any case, it is important to know when a problem develops. Traffic-monitoring devices can often alert administrators to emerging problems that can be addressed before they become critical.

LAN-to-WAN Traffic and Performance Monitoring and Analysis

Monitoring the traffic that flows through the LAN-to-WAN Domain can be a demanding task, but it is one that is a vital part of ensuring your environment's security. A secure network is one that provides smooth operation and allows only authorized traffic. If any part of your network were to be down even for a small period of time, productivity within your organization would decline. In the case of critical business functions, network problems could cause service interruptions and could result in noncompliance. To be proactive, it is important to monitor how traffic moves throughout the network and to verify that your network is meeting your organization's security goals.

Traffic monitoring and analysis is the process of capturing network traffic and examining it to determine how users and applications are using your network. The two main monitoring techniques are network device based and non-device based. Network devices, especially routers and gateways, often include monitoring functionality you can use to keep track of your network's health. Non-device techniques require that you add hardware or software to capture traffic and analyze it. Any computer in the LAN-to-WAN Domain can act as a traffic-capture device.

After you capture traffic, your analysis software can examine it in real time or save it to a file for later analysis. Monitoring and analyzing network traffic in the LAN-to-WAN Domain is very similar to monitoring and analyzing traffic in the LAN Domain. The goal is to detect problems before they become critical. Your efforts should focus on identifying degrading performance that might affect data availability or traffic that might indicate attack activities.

LAN-to-WAN Configuration and Change Management

The LAN-to-WAN Domain exists to provide a structured transition between your LAN and a

WAN, such as the Internet. Much of the functionality in the LAN-to-WAN Domain depends on the configuration of the devices in the domain. Each device or software component operates based on configuration settings and rules. Any change to settings or rules changes the way the domain components operate.

After you configure the components in the LAN-to-WAN Domain to operate securely, it is important to prohibit unauthorized changes to the domain configuration. Any configuration changes you make will change the way components operate. Changes can be beneficial or detrimental. You must enforce a change-management process to ensure you only make authorized changes to any configuration and that you document all changes for later auditing.

The change-management process is fairly simple and contains only a few steps. Each step is important and contributes to the overall security of your environment. Here are the basic configuration-management steps required to make any changes to device configuration settings or rules:

1. The requestor submits a configuration setting or rule change request. It is important to document each change and the reason for the change. Auditing configuration changes and comparing the impact of similar changes requires as much historical information as possible.
2. The **configuration control board (CCB)** reviews each request and either approves or denies it. The CCB can be a group of people or a single person with the responsibility to evaluate changes.
3. The implementers—generally security administrators—receive approved change requests for implementation and make the approved changes.
4. Before making any changes, security administrators should validate the current configuration against the latest authorized baseline. This step identifies any unauthorized changes.
5. Security administrators should validate any configuration changes in a test environment whenever possible.
6. After applying authorized changes, security administrators should create a new authorized baseline.
7. The implementers should validate the changes made to ensure they satisfy the original request.

Coordinated Attacks

Many attacks against enterprise data really consist of multiple coordinated attacks. Suppose an attacker wants to launch a DoS attack to disable your organization's Web servers and stop you from conducting business on the Internet. The attacker attempts a direct DoS attack that your IPS devices in the LAN-to-WAN Domain immediately identify and stop.

The attacker searches for other vulnerabilities and finds a way to use social engineering to install a Trojan horse on the IPS device. The Trojan horse provides a back door that the attacker can use to log on to the IPS and change configuration settings. The attacker modifies the IPS rules to not block the attacking computers. The next attack succeeds in bringing down your Web servers. This attack is successful because of a lack of controls at several levels. The last level of control that is missing is positive configuration management for the IPS.

Although it might seem like an intrusive process, requiring all configuration changes to go through a change-management procedure allows you to audit all authorized changes and

deploy only approved changes. The overall configuration-management process should also include periodic audits of each component's configuration against the latest baseline to identify unauthorized changes. In this way, you can ensure your LAN-to-WAN components maintain a secure configuration.

LAN-to-WAN Management, Tools, and Systems

Managing the LAN-to-WAN environment basically involves the same tasks as managing the LAN environment. In addition, managing the LAN-to-WAN environment involves efforts to ensure the additional components in the LAN-to-WAN Domain are protecting the internal domains from the external domains. The LAN Domain, as the name implies, focuses on LAN-specific topics. The LAN-to-WAN Domain includes WAN access components and security needs.

Managing the LAN-to-WAN Domain means ensuring authorized data passes smoothly through the domain's components and on to its destination. This means ensuring you have defined just the right firewall rules. Use the principle of least privilege to write firewall rules. Your rules should allow through the firewall only the traffic that is necessary to perform authorized business functions. In today's distributed environments, that goal is difficult to achieve. Users and applications tend to establish and use multiple connections with remote services and resources. Your firewall rules should allow all of the different connections you'll need and can take some fine-tuning to get right.

FCAPS

Managing a network involves several related tasks and can become confusing without a plan. The **International Telecommunication Union Telecommunication Standardization Sector (ITU-T)** (one of three divisions of the International Telecommunication Union, primarily responsible for communications standards) and the International Organization for Standardization (ISO) developed **FCAPS**. FCAPS is a network-management functional model. FCAPS is an acronym that represents the focal tasks necessary to effectively manage a network. FCAPS stands for the following:

- **Fault management**—This includes activities to detect, log, communicate, and potentially fix network problems to keep the network running effectively. Fault management directly addresses the availability property of security by minimizing downtime.
- **Configuration management**—This includes activities to monitor network component configuration settings to track and manage the state of your network.
- **Accounting management**—This includes activities to measure how your users are using your network to support regulation compliance and billing.
- **Performance management**—This includes activities to measure and report on network performance to support optimization.
- **Security management**—This includes activities to control access to network resources and limit access exclusively to authorized users.

Network-Management Tools

Many tools are available to help manage your network. Look for the tools that best fit into your environment and provide the functionality you need to best manage your environment.

Table 11-1 shows a list of a few network-management products.

Although these tools represent functionality that is useful in the LAN-to-WAN Domain, many of them are useful to manage networks in other domains as well. Select the tools that work best to help keep your networks secure and operating smoothly.

Access Rights and Access Controls in the LAN-to-WAN Domain

In the context of the LAN Domain, your organization can exert substantial control over which computers and users can establish connections. The situation is slightly different in the LAN-to-WAN Domain. Although it is still possible to require strict access controls, the design of the LAN-to-WAN Domain includes active connections to a WAN. That means the components in this domain are exposed to the WAN, which in many cases is the Internet.

Internet-facing components are network components in your organization's IT infrastructure that users can access via the Internet. These components experience a higher number of threats due to this increased visibility. To make matters worse, many enterprise applications that provide Internet connectivity encourage at least some anonymous connections. This exposure to anonymous users makes it more difficult and more important to secure the components in the LAN-to-WAN Domain.

The transitional nature of the LAN-to-WAN Domain calls for collections of controls to meet security needs. You need the ability to evaluate several attributes of a connection request's source before granting access to your network. You should define different access profiles based on your policies to meet the needs of different types of network users. **Network Access Control (NAC)** is a solution that defines and implements a policy that describes the requirements to access your network. NAC defines the rules a connecting node must meet to establish a secure connection with your network. It also allows you to proactively interrogate nodes that request a connection to your network to ensure they don't pose a risk. You can use NAC to classify connecting nodes based on the level of compliance with your access rules. NAC allows you to evaluate node attributes that include the following:

- Anti-malware protection
- Firewall status and configuration
- Operating system version and patch level
- Node role and identity
- Custom attributes for enterprise configuration

TABLE 11-1 Network-management tools.

FCAPS AREA	TOOL	SOURCE
Fault management	Nagios (open source and commercial)	http://www.nagios.org/
Fault management	OpenNMS (open source)	http://www.opennms.org/
Fault management	NMIS (open source)	http://www.sins.com.au/nmis/
Configuration management	RANCID (open source)	http://www.shrubbery.net/rancid/
Configuration management	Canner (open source framework)	http://bangj.com
Accounting	Lightweight Directory Access	Supported by many software products and

management	Protocol (LDAP)	available for most operating systems
Accounting management	Terminal Access Controller Access Control System (TACACS)	Supported in most current operating systems
Accounting management	Remote Authentication Dial-In User Service (RADIUS)	Supported in most current operating systems
Performance management	Cacti (open source)	http://www.cacti.net/
Performance management	SmokePing (open source)	http://oss.oetiker.ch/smokeping/
Performance management	PRTG (open source)	http://www.paessler.com/prtg/
Performance management	MRTG (open source)	http://oss.oetiker.ch/mrtg/
Security management	Windows Firewall	Microsoft Windows operating systems
Security management	IPtables	Most Linux distributions
Security management	Vendor-specific firewall device	Each vendor provides specific software for its own network devices

Allow Anonymous Users?

Enterprise Web-based applications generally share a common problem: How do you attract new customers to your product line before you know who they are? Historically, merchants would use advertising to send information out to prospective customers. Today's model encourages prospective customers to visit online resources. Most online merchants allow casual, anonymous users to browse their Web sites and learn more about their products. Your security controls in the LAN-to-WAN Domain must provide access for these anonymous users while still ensuring the security of your data. Solid access controls can help you meet that goal.

NAC solutions enable you to exert control over which nodes can connect to your networks and what rights you'll grant to them once they connect. NAC provides a formal method to establish relationships with several types of security controls and helps you minimize threats from malware, increase LAN-to-WAN availability, and provide proof of compliance through NAC-related auditing data. NAC is a developing approach to controlling network access that several vendor products support. [Table 11-2](#) lists some vendors that provide NAC software.

You can choose from many products to implement NAC. NAC software alone won't secure your networks, but it does give you the ability to define and enforce policies that can get you closer to your security goals.

TABLE 11-2 NAC software products.

PRODUCT	WEB SITE
PacketFence (open source)	http://www.packetfence.org/en/home.html
Sophos NAC Advanced	http://www.sophos.com/products/enterprise/nac/sophos-nac/
Symantec Network Access Control	http://www.symantec.com/business/network-access-control
Cisco Network Admission Control	http://www.cisco.com/c/en/us/solutions/enterprise-networks/network-admission-control/index.html

Maximizing C-I-A

As with all other domains in the IT infrastructure, your main goal in the LAN-to-WAN Domain is to deploy and maintain controls that support all of the C-I-A properties of security for your data. The LAN-to-WAN Domain contains several components that play critical roles in providing secure access to your organization's data. Maintaining that security requires diligence and the right controls.

Minimizing Single Points of Failure

One of the main functions of the LAN-to-WAN Domain is to provide access, or connectivity, between the LAN and the WAN domains. One property in the C-I-A triad is availability. Resources and data are available only if users can successfully establish connections between the two domains. If any device in the LAN-to-WAN Domain is required to make a connection, that device must be functional 100 percent of the time to fully support data availability. Any downtime will affect the security of your environment.

To minimize any downtime due to device failure in the LAN-to-WAN Domain, ensure every node has an alternate whenever possible. Any node that does not have an alternate becomes a single point of failure. If the node fails or becomes unavailable, it affects the entire domain. Evaluate each node to see if a redundant node would remove the single point of failure. Allow unique devices only if there are no other available alternatives and implement compensating controls to protect the availability property.

Dual-Homed ISP Connections

Many organizations employ a single connection to their ISP. If the connection device goes down, so does the Internet access for the entire organization. In the preceding section, you learned to avoid single points of failure. That goal applies to your ISP connection as well. The solution is to establish at least two ISP connections, as shown in [Figure 11-7](#). A **dual-homed ISP connection** is a design in which a network maintains two connections to its ISP. If one gateway or connection fails, the other can still connect to the Internet.

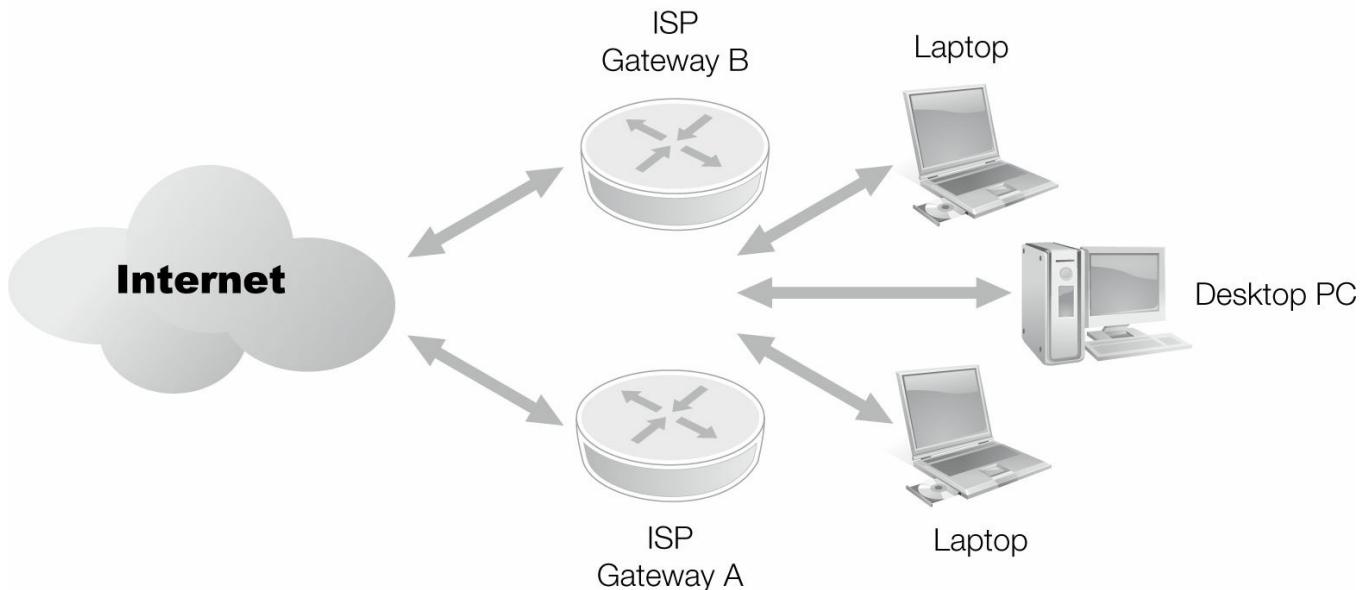


FIGURE 11-7 Multiple ISP connections avoid a single point of failure.

FYI

Methods of choosing which ISP connection to use can be very simple. The round-robin method simply keeps a list of all available ISP connections. When you use one connection, the system remembers to use the next connection in the list the next time someone wants to connect. When you reach the end of the list, just start over. This method cycles through the list of ISP connections over and over.

The other simple method is to remember the number of times you have used each ISP connection. When a user wants to connect to an ISP, you select the connection with the lowest number of uses. This simple method helps you use all of your connections equally.

In the simplest case, you use the primary connection for normal Internet access. You use the secondary connection only if the primary connection fails. You can implement this solution easily, but it does waste the available bandwidth on the secondary connection because it sits unused most of the time. Another option is to use both connections at all times. Your ISP connection devices can decide which connection to use based on many criteria. More-sophisticated connection-management software can use the best ISP connection based on available bandwidth. This provides load balancing as well as fault tolerance. Less-sophisticated connection-selection methods may involve simple round-robin or connection-count algorithms. Regardless of the method you use, having a secondary ISP connection can protect you from WAN connection failures.

If you decide to set up dual-homed ISP connections, you can choose from two different options:

- **Use two connections to the same ISP**—Two connections to the same ISP might save money but are still vulnerable to interruption if your ISP fails.
- **Use two connections to different ISPs**—Maintaining two connections to different ISPs will cost more and require more maintenance due to working with different vendors, but will protect your environment if one ISP goes down.

Examine using dual-homed ISP connections to maximize your data availability.

Redundant Routers and Firewalls

A common bottleneck in any network is the router or firewall. In many networks, these devices require that all traffic pass through them. Although that practice does make maintenance and configuration easier, it introduces one or more single points of failure. If all traffic from the Internet passes through one router and that router crashes, how can your Internet users connect to you? The answer is, they can't.

The easiest way to see the most obvious single points of failures for network connections is to map your network. It is easy to see on a network map where node failure would result in a fragmented network. After you identify routers and firewalls that are single points of failure, you should introduce redundant nodes to your network. Every single point of failure should have at least one alternate device. Having redundant devices allows your network to continue in the case of a device failure. If there are two paths from point A to point E and one path fails, all traffic can use the other path. Implementing redundant devices addresses availability by protecting your network from device failure. In addition, you gain the additional benefit of spreading out traffic among the redundant devices and possibly increasing overall performance. In both cases, redundant network devices can protect the availability of your network.

Web Server Data and Hard Drive Backup and Recovery

You should have a recovery plan in place for every device and computer in your organization. **Business continuity plans (BCPs)** and **disaster recovery plans (DRPs)** enable you to recover from disruptions ranging from small to large.

One crucial part of a BCP or a DRP involves recovering data and configuration settings from a secondary copy saved in case you lose your primary copy. This secondary copy of data to be used in case of primary data loss is commonly called a *backup image* of data, or just a *backup*. The value of a backup in the recovery process depends on how current it is. Because you'll lose any work that occurred after your last backup when you recover data, it makes sense to back up frequently.

One of the more common servers in the DMZ is the Web server. Web servers provide a generic front end to many enterprise applications and resources. Web servers provide the first visible point of contact for many remote clients and are necessary to bridge the outside Internet user community with the far more structured collection of application components in your organization's secure network. If your organization's Web server is down, your organization's Web presence is down, too. To maximize the availability of your organization's Web presence even in the face of disasters, it is important to ensure you have a current recovery plan for all the Web servers in the LAN-to-WAN Domain. A current recovery plan is one that you support with frequent backups—and one that you test on a regular basis. A solid schedule for backups and a plan to recover your Web servers in the case of an interruption that involves data loss will maximize your organization's uptime.

Use of Virtual Private Networks for Remote Access to Organizational Systems and Data

You have seen several topics that relate to data availability but nothing yet that relates to the other two properties of the C-I-A triad, integrity and confidentiality. Information that travels to and from the Internet or another WAN can potentially be accessed by pretty much anyone. The best protection for information on a WAN is to use encryption. You can allow remote users to access resources on your LAN through the LAN-to-WAN Domain by setting up a **virtual private network (VPN)**.

A VPN is a persistent connection between two nodes. The nodes can be on the same network or on separate networks. Many VPNs also encrypt all the traffic that flows along the connection. Because the traffic is encrypted, no unauthorized users can see the information. In this manner, encryption supports data confidentiality. Attackers can modify the data along its route, but without knowing what the data actually contains, the changes would not have a real purpose other than to destroy data. When the altered data reaches the end of the VPN and is decrypted, the VPN endpoint detects the change and takes action. The endpoint can either request that the data be resent or throw an error. Either way, you detect the unauthorized change and protect the data's integrity.

 **NOTE**

VPNs provide secure access to remote users and are particularly pertinent to the Remote Access Domain.

Penetration Testing and Validating LAN-to-WAN Configuration

Testing security controls and configuration settings is crucial to ensuring you have the right controls in place. One particular type of testing simulates actions an attacker would take to attack your network. This type of test is called a *penetration test* because the purpose of the test is to attempt to penetrate, or compromise, your security controls. In fact, conducting periodic penetration tests is a requirement for compliance with several standards. PCI DSS is one example of a standard that requires annual penetration tests to validate security controls.

An experienced penetration tester can simulate the actions an attacker would take and verify the strength of your security controls. Such tests validate the controls you have in place as well as indicate areas of weakness you should address. You should seek approval first, then design several types of penetration tests to ensure your security controls are doing the job.

Never conduct a penetration test unless you have written authorization from the network and system owners. Penetration tests will likely raise alarms. If you're not authorized to perform the tests, it could result in liability issues and even criminal prosecution. Verbal approval is not enough—get it in writing. Before you start any penetration testing, get written approval for the specific scope of your tests. Your approval documents should include the following:

- Specific IP addresses or ranges of nodes you will test
- Specific IP addresses of nodes that will conduct the tests
- A list of nodes that should be excluded from the tests
- A list of the techniques used in the tests
- A schedule or time frame approved for the tests to occur
- Points of contact for the testing team and the approving organization(s)
- Procedures for handling collected test data

External Attacks

The more common type of penetration test is from the perspective of the external attacker. The penetration tester, also called the *pentester*, launches a series of attacks from outside the

target's network. In most cases, the pentester conducts the tests from a computer connected to the Internet. The tester simulates the actions an attacker would take when developing an attack on your organization.

Although each penetration test is different, many tests follow similar paths. Here is a common flow a penetration tester follows to develop attacks:

- 1. Reconnaissance**—Here, the tester collects as much information about the target environment as possible. At this stage, the tester is collecting both technical and nontechnical information. Both types of information can help the tester determine how the organization operates, where it operates, and which characteristics the organization and its customers value. The purpose of the attack will drive the process. In an actual attack, if an attacker wants to extract or modify data, all efforts will be directed toward the data of interest. If the attacker wants to harm the organization, the target of the attacks will be what the organization values. An organization that markets safety to its clients would suffer from confidential data disclosure, whereas an organization that prides itself on high availability would suffer most from being shut down. Information gathered by the tester or attacker in the reconnaissance phase drives all subsequent activities.
- 2. Footprinting**—After collecting general organizational information, the next step is to learn as much as possible about the target's technical architecture. At this point, testers use tools to query and identify as many identified nodes in the target network as possible. The process of **footprinting** means determining the operating system and version for each node. Operating system information helps identify a node's possible purpose and the next steps to learn more about the node.
- 3. Scanning and enumeration**—The next step collects detailed information about each node. Testers can use automated tools to scan each node, identifying open and active ports. Testers can also query open ports to determine which services are running on a selected node. In this manner, testers can develop a detailed map of the target's technical environment and get a good picture of what hardware and software make up the target's infrastructure.
- 4. Vulnerability identification**—Once the testers have all the available information on operating systems and running software and services, the next step is to explore known vulnerabilities in the target's environment. For example, if scanning and enumeration reveals the target is running Microsoft Internet Information Services (IIS) Web server version 6.0, the testers would search for known vulnerabilities with that specific version.
- 5. Attack planning**—A complete attack plan would include all identified vulnerabilities in the target environment, sorted by exploit difficulty and impact. In most cases, testers will start with the easiest attacks that produce the largest impact. The attack plan is a sorted list of attacks that the testers will carry out along with the procedures to execute the attack and collect results information.
- 6. Attack execution**—The execution phase follows the attack plan and launches each attack against the target environment. Testers grade the success of each attack and the effectiveness of security controls to mitigate the attack.
- 7. Collecting and presenting results**—The final step in a penetration test is to compare the attack plan with the attack results. Testers will collect all result information from each attack and present a report of overall test performance. The report should analyze the effectiveness of existing controls and make recommendations for any changes that would increase security.

Internal Attacks

Not all attacks occur from external sources. Many attacks originate from within an organization's own networks. These types of attacks can originate from compromised computers running malware or from attackers who have bypassed access controls and gained a foothold inside your network. In either case, attacks from within your organization can be more dangerous than attacks from the outside.

Internal traffic and activities are generally regarded as more trusted than external traffic. The general idea is that if a user has successfully satisfied stringent access controls, that user should be trusted. This general trust makes internal attacks dangerous if an attacker is able to circumvent access controls and operate from within your internal networks.

To measure your organization's ability to handle internal attacks, you should conduct internal penetration tests as well as external tests. There are two main types of attacks that may originate from within your organization:

- **Internal attacks on your organization**—An **internal attack** is one in which an attacker is able to compromise your access controls and either establish a presence inside your networks or place malware on an internal computer. In either case, the attacker has access to your resources at a higher level of trust than a general external user. Internal attacks generally target your organization.
- **Internal-to-external attacks on another organization**—An attacker might choose to use your infrastructure to launch an **internal-to-external attack** on another organization. There are two main reasons for using one organization to attack another. First, an attacker could use your organization to launch an attack in an attempt to hide the attack's true origin. Second, the main goal of the attack could be to place the blame on your organization and cause you to incur embarrassment and possibly other consequences.

Regardless of the reasons, internal penetration testing exercises your security controls to ensure both types of attacks will not succeed. Your goal is to ensure internal attacks on your organization will not compromise your security and attacks on other organizations will not be allowed past your networks. Both external and internal penetration testing ensure your environment is secure from attacks in both directions.

Intrusive Versus Nonintrusive Testing

Penetration tests are simulations of attacks. In most cases, attacks on information systems and infrastructures are intended to cause damage of some sort. That means if you fully simulate attacks, there will likely be some impact that results. Any test that simulates an attack and results in damage is an **intrusive test**. A test that only validates the existence of a vulnerability is a **nonintrusive test**.

For example, suppose your organization runs the Apache Web server. Penetration testers discover a vulnerability in the version of Apache running on your primary Web server. The vulnerability, if exploited, will cause the Web server to crash. Scanning and enumerating your Web server computers to collect data is generally a nonintrusive test, whereas exploiting the vulnerability and actually crashing the Web server is an intrusive test.

As you develop a penetration plan, assess the impact of each test and carefully consider whether you want to allow intrusive tests against your environment. If all your security controls are sufficient, even intrusive tests will fail to affect your environment. But any deficiency in your controls could allow an intrusive test to have a negative impact on your

systems or networks. The best way to handle such intrusive tests in a safe manner is to perform them against a test environment that is an exact copy of your production environment.

TIP

Although creating a test environment takes substantial effort, today's use of virtualization can make the process far easier. You can create a collection of virtual machines that replicate your real environment and provide a good test bed for penetration testing.

Configuration Management Verification

You learned about the importance of managing network information earlier in this chapter. Recall the FCAPS approach to network management. The C in FCAPS stands for configuration. You also saw two tools in [Table 11-1](#), RANCID and Canner, that help manage network configuration settings. It is important to aggressively control your network devices' configuration settings. RANCID and Canner, along with other available tools, can help you create baselines of configuration settings and compare changes over time. You should develop a schedule and process to frequently compare configuration baselines and verify all changes to your network's configuration.

A solid network configuration-management process makes it easy to classify any configuration changes as authorized or unauthorized. You just compare baseline differences to your authorized changes list to see which changes occurred that were not authorized. Because every configuration change has some effect on what traffic flows through your LAN-to-WAN Domain, it is important to manage authorized changes and detect any unauthorized changes. Implementing the FCAPS approach will help formalize the process and make your networks more secure.

Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines

Compliance in the LAN-to-WAN Domain depends on implementing the best controls. As with other domains, explore alternative controls for each security goal. Many of the LAN-to-WAN security controls affect performance and the ability of your users to access your organization's resources. You must ensure the correct controls are in place to balance all three security properties.

As you analyze controls in the LAN-to-WAN Domain to meet compliance requirements, ensure each control satisfies your security policy. If a control does not support any part of your security policy, you should question its value to your organization. Although various legislation, regulations, and vendor standards have different requirements, [Table 11-3](#) lists the types of controls for which you'll likely need to ensure compliance in your LAN-to-WAN Domain.

Implementing multiple types of controls decreases the likelihood an attack will be successful and makes your LAN-to-WAN Domain more secure.

Best Practices for LAN-to-WAN Domain Compliance

The LAN-to-WAN Domain provides the outside world with access to your data. In many ways, the domain filters authorized users from unauthorized ones. Because this domain connects your secure LAN with an untrusted WAN, you must ensure the controls protect your LAN resources. Protecting information in the LAN-to-WAN Domain focuses on maintaining the balance between easy access and solid security. Solid planning, along with aggressive management, can provide both.

The following best practices represent what many organizations have learned. Plan well and you can enjoy a functional LAN-to-WAN Domain that makes LAN information available for use to WAN users. Here are general best practices for securing your LAN-to-WAN Domain:

- Map your proposed LAN-to-WAN architecture before installing any hardware. Use one of the several available network-mapping software products to make the process easier. Identify all of the components' data paths through the domain. Use the map to identify any single points of failure. Update the network map any time you make physical changes to your network.
- Establish a DMZ with at least two firewalls. You should locate one firewall between your WAN connection and the DMZ perimeter and configure it to filter incoming and outgoing traffic between the WAN and the DMZ. Locate the other firewall between your LAN and the DMZ. This internal firewall should filter all incoming and outgoing traffic between the LAN and the DMZ.

TABLE 11-3 Common compliance controls in the LAN-to-WAN Domain.

TYPE OF CONTROL	COMPONENT	DESCRIPTION
Preventive Controls	DMZ	Use firewalls to separate resources in the LAN-to-WAN Domain from both the WAN and your LAN. A well-configured DMZ prevents unauthorized WAN users from accessing resources in your LAN.
	Firewalls	Implement firewalls between any LAN-to-WAN boundaries to filter out unauthorized traffic. A more aggressive approach is to implement firewalls between servers in the LAN-to-WAN Domain as well as on the domain boundaries.
	Network address translation (NAT)	Use NAT to hide internal IP addresses from the outside world.
	Intrusion prevention system	Use at least one IPS for each ISP connection to detect and prevent intrusions.
	User-based access controls for DMZ resources	Restrict access to DMZ resources to reduce what WAN users can access.
	Configuration change control	Limit changes to network device configuration settings and filtering rules. Require approval for all changes before deploying them.
	Encryption	Enforce encryption for all connections that span the LAN-to-WAN Domain, involve elevated authorization, or transport sensitive data of any kind.
Detective Controls	Service exception auditing	Log failures for all service consumption requests. Failed service requests could be the signs of either an attack or reconnaissance for a future attack.
	Performance monitoring	Frequently sample network traffic flow metrics and be alert for any unusual activity.

	Packet analysis	Examine packets for known attack signatures and to ensure necessary data is encrypted.
	Configuration settings monitoring	Compare LAN-to-WAN device configuration settings to stored baselines to detect any unauthorized changes.
	Intrusion detection system	Use at least one IDS for each ISP connection to detect intrusions.
	Penetration testing	Conduct periodic penetration tests to identify security control weaknesses.
Corrective Controls	Operating system and application patching	Keep applications and operating systems patched to the latest available level.
	Attack intervention	Automatically modify filtering rules to deny traffic from sources generating known attack signature packets.
	BCP and DRP	Develop and maintain plans to survive and continue operations in the face of small or large disruptions.

- Implement at least two redundant WAN connections. Use load-balancing techniques to use the bandwidth of both connections.
- Configure all DMZ servers and devices to resist attacks from WAN users.
- Develop a backup and recovery plan for each component in the LAN-to-WAN Domain. Include recovery plans for damaged or destroyed connection media. Don't forget to include configuration settings for network devices in your backup and recovery plans.
- Implement frequent update procedures for all operating systems, applications, and network device software and firmware.
- Define routing and filtering rules to restrict traffic passing through the LAN-to-WAN Domain. Most traffic should either terminate or originate in the LAN-to-WAN Domain.
- Monitor LAN-to-WAN traffic for performance and packets for suspicious content.
- Carefully control any configuration setting changes or physical changes to domain nodes. Update your network map after any changes.
- Use automated tools whenever possible to map, configure, monitor, and manage the LAN-to-WAN Domain.
- Deploy at least one IPS for each WAN connection to detect and respond to suspected intrusions.
- Conduct complete penetration tests at least annually to evaluate security control effectiveness.

As with all best practices, these are only a starting point. Implement the points that are appropriate for your environment. Doing so will get you started toward establishing and maintaining a secure LAN-to-WAN Domain.



CHAPTER SUMMARY

In this chapter, you learned about how the LAN-to-WAN Domain provides WAN users with access to your organization's LAN resources. Although it is important to secure your

organization's information from internal users, it is equally important to protect your resources from attacks from WAN users. You learned about the components commonly found in the LAN-to-WAN Domain and the importance of monitoring and configuring components properly. You learned about some of the most important security controls and how to maximize C-I-A in the LAN-to-WAN Domain.

Much of an organization's high-value information resides in the LAN Domain. The LAN-to-WAN Domain exposes that information to many WAN users. Security controls in the LAN-to-WAN Domain are crucial to protect information from threats. Solid controls and management procedures can make your organization's information available to the largest number of potential users with the minimum amount of risk.



KEY CONCEPTS AND TERMS

Business continuity plans (BCPs)
Configuration control board (CCB)
Data leak security appliances
Demilitarized zone (DMZ)
Disaster recovery plans
Distributed applications
Dual-homed ISP connection
FCAPS
Firewall
Footprinting
Honeypot
Internal attack
Internal-to-external attack
International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
Internet service provider (ISP)
Intrusion detection system (IDS)
Intrusion prevention system (IPS)
Intrusive test
LAN-to-WAN Domain
Multiprotocol Label Switching (MPLS)
Network Access Control (NAC)
Nonintrusive test
Proxy server
Service
Single point of failure
Traffic-monitoring devices
Virtual private network (VPN)



CHAPTER 11 ASSESSMENT

1. A distributed application is one in which the components that make up the application reside on different computers.

 - A. True
 - B. False
2. Which of the following is commonly the primary security control for data entering the LAN-to-WAN Domain?

 - A. Filtering
 - B. NAT
 - C. Encryption
 - D. Address validation
3. A(n) _____ makes requests for remote services on behalf of local clients.
4. A(n) _____ is an isolated part of a network that is connected both to the Internet and your internal secure network and is a common home for Internet-facing Web servers.
5. Which type of network device is most commonly used to filter network traffic?

 - A. Router
 - B. Firewall
 - C. Switch
 - D. IDS
6. If you only have one connection to the Internet and that connection fails, your organization loses its Internet connection. This is an example of a(n) _____.
7. Which of the following devices detect potential intrusions? (Select two.)

 - A. Firewall
 - B. IPS
 - C. IDS
 - D. Load balancer
8. What does it mean when there are differences between the last security configuration baseline and the current security configuration settings?

 - A. Unauthorized changes have occurred.
 - B. Authorized changes have occurred.
 - C. Changes have occurred (either authorized or unauthorized).
 - D. Unapproved changes are awaiting deployment.
9. Which of the following is a solution that defines and implements a policy that describes the requirements to access your network?

 - A. NAC
 - B. NAT
 - C. NIC
 - D. NOP
10. Which of the following best describes a dual-homed ISP connection?

 - A. An ISP connection using two firewalls
 - B. Connecting two LANs to the Internet using a single ISP connection
 - C. A network that maintains two ISP connections
 - D. Using two routers to split a single ISP connection into two subnets
11. Many organizations use a(n) _____ to allow remote users to connect to internal network resources.
12. You only need written authorization prior to conducting a penetration test that accesses resources outside your organization.

 - A. True
 - B. False
13. NAT is helpful to hide internal IP addresses from the outside world.

- A. True
- B. False

14. The _____ feature speeds up routing network packets by adding a label to each packet with routing information.

15. Which of the following best describes the term *honeypot*?

- A. A server that is deliberately set up in an unsecure manner to attract attackers
- B. A server that contains extremely sensitive data
- C. A collection of computers that are vulnerable to attack and could allow your network to be compromised
- D. Vulnerable servers in your network that would not be dangerous if compromised

CHAPTER 12

Compliance Within the WAN Domain

T

ODAY'S ORGANIZATIONS depend on a workforce that is mobile and widely dispersed.

Work has to get done regardless of where the workers might be at any one moment. An IT infrastructure that supports this type of mobility and flexibility has to include the ability for workers to connect from almost anywhere. Organizations are deploying resources and applications that are easier than ever to access from remote locations. These organizations need a framework to describe how to provide access to the organization across town or across the world—and to do it securely.

In this chapter, you'll learn about what happens to data in the WAN Domain and how you can ensure compliance as your data travels outside your environment.

Chapter 12 Topics

This chapter covers the following topics and concepts:

- How compliance law requirements relate to business drivers
- Which devices and components are commonly found in the WAN Domain
- What WAN traffic and performance monitoring and analysis are
- What WAN configuration and change management are
- Which WAN management tools and systems are commonly used
- What access rights and access controls in the WAN Domain are
- How to maximize C-I-A
- What WAN service provider SOC compliance is
- How to ensure adherence to documented IT security policies, standards, procedures, and guidelines
- What best practices for WAN Domain compliance are

Chapter 12 Goals

When you complete this chapter, you will be able to:

- Examine compliance law requirements and business drivers
- Compare how devices and components found in the WAN Domain contribute to compliance
- Describe methods of ensuring compliance in the WAN Domain
- Summarize best practices for WAN Domain compliance

Compliance Law Requirements and Business Drivers

Organizations rely on distributed architectures. Many organizations deploy their enterprise applications as distributed applications. Although the actual applications and resources belong in other domains, clients need the ability to access resources and run distributed programs. Providing the ability to connect diverse resources is the main purpose of the WAN Domain. Although making your resources and data available to more users is a good thing, you must pay close attention to security. Keeping your data secure as it leaves your network takes advance planning. Always consider how secure your data is in each of the domains of your IT infrastructure. [Figure 12-1](#) shows the WAN Domain in the context of the seven domains in the IT infrastructure.

Your responsibility to keep your data secure doesn't stop when that data leaves the controlled area of your networks. The WAN Domain represents an area that might be largely out of your control, however. Your responsibility to secure data means to protect it in such a way that it is secure even when traveling across an untrusted network. Ensuring data is safe even in the WAN Domain makes it possible for your organization to deploy distributed applications that can provide unprecedented functionality to remote users. Implementing the controls necessary to support your security policy in the WAN Domain makes your organization more secure and allows you to provide a higher level of visibility to your data.

Protecting Data Privacy

WANs provide the valuable service of connecting your networks together without having to install or maintain the interconnection network media. In other words, you use someone else's network to connect your networks together. You can connect your headquarters to several branch offices using a WAN. You connect each of your networks to the WAN and all your nodes can communicate. The only problem is that you now depend on another organization to communicate. Each time you send a message from your headquarters to a branch office, that message travels across someone else's network. You no longer have control over who sees your network traffic or who can alter it. [Figure 12-2](#) shows how data traveling from one of your nodes to another across a WAN is out of your control.

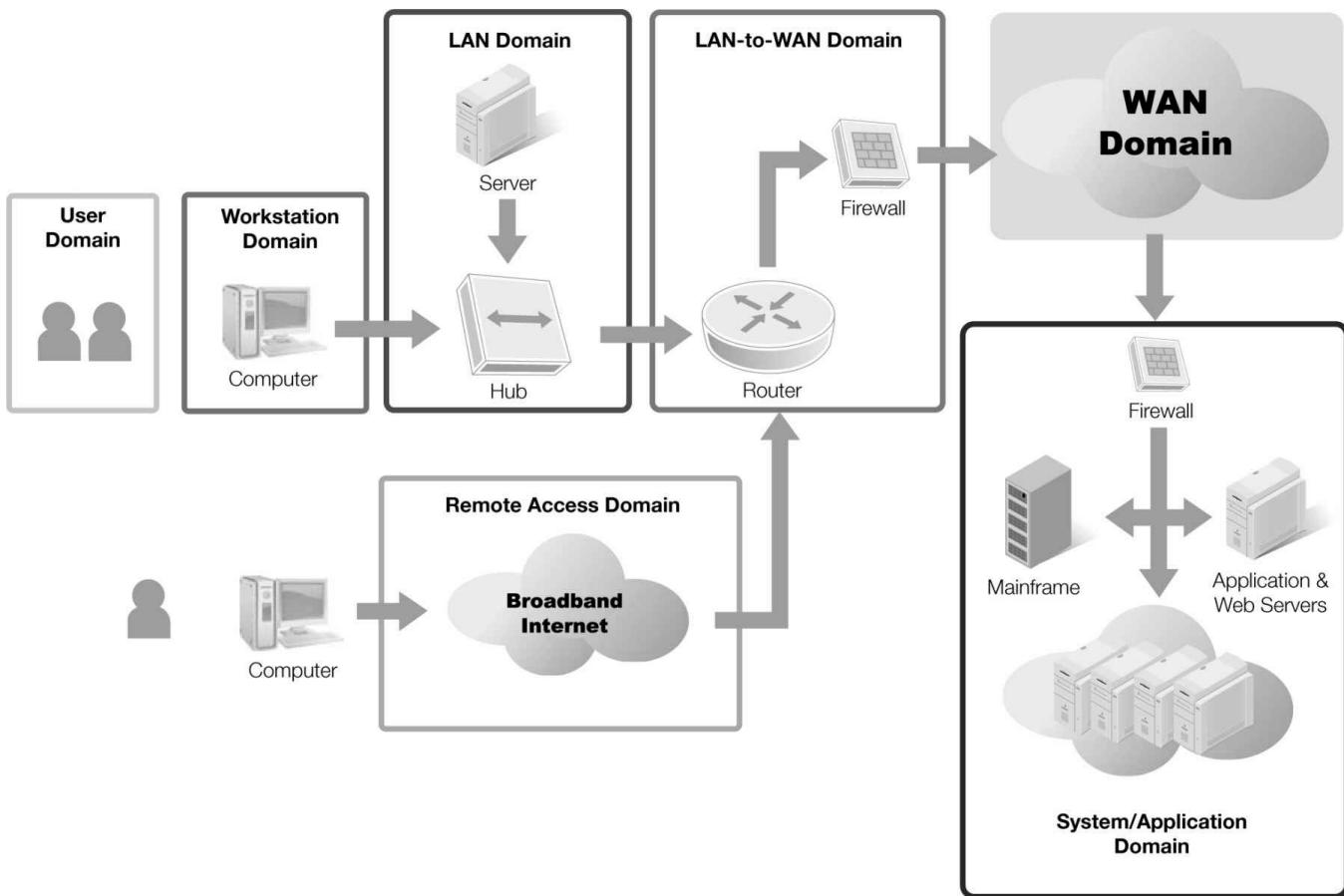


FIGURE 12-1 The WAN Domain within the seven domains of a typical IT infrastructure.

Cloud Computing

Recently there has been a movement to cloud computing. The word cloud, however, can take many different meanings and depends upon the cloud model. The National Institute of Standards defines cloud computing as “a model for enabling ubiquitous, 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.” The three common service models include delivering infrastructure, complete platforms, or simply software as a service. Compliance with the WAN Domain should certainly consider cloud solutions. On a related note, cloud services are changing how distributed networks are managed and delivered.

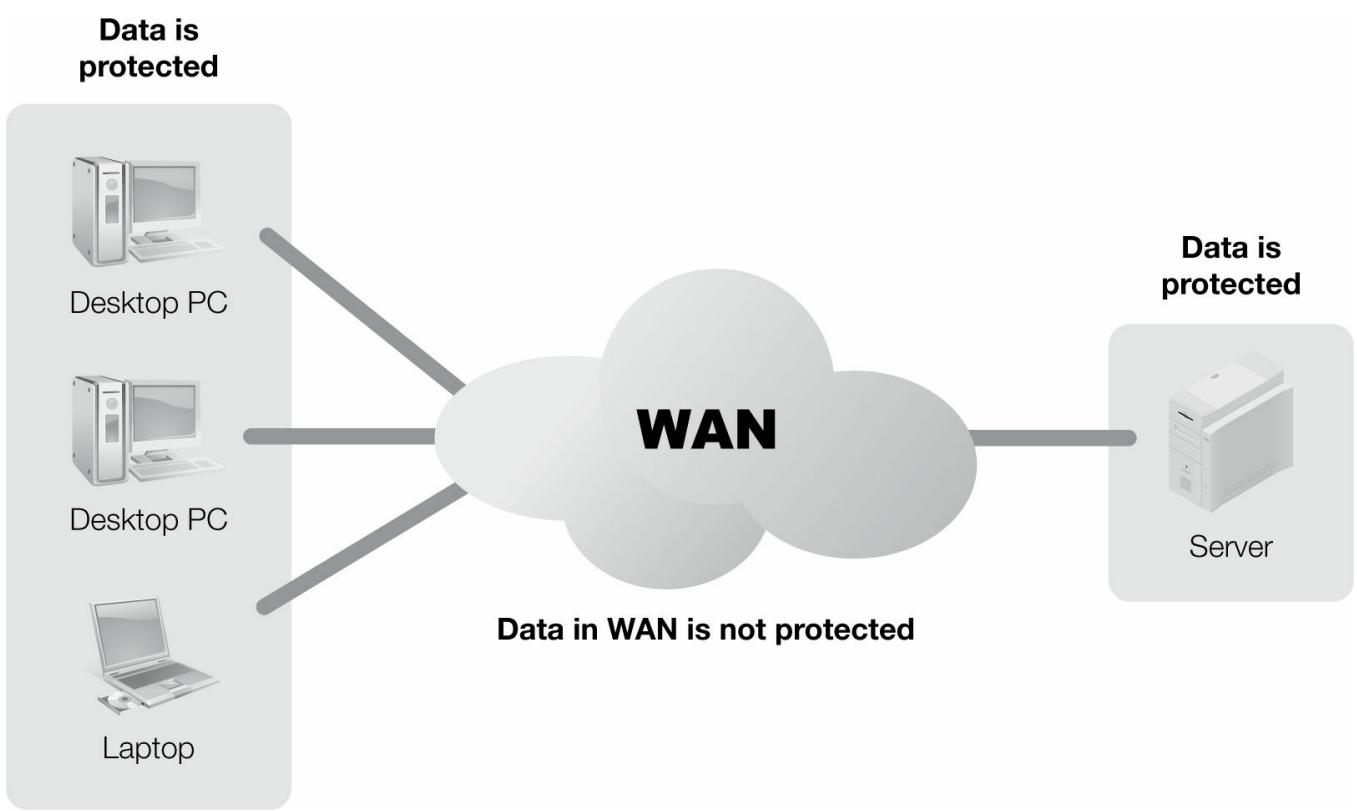


FIGURE 12-2 Lack of control for data traveling across a WAN.

One of the most important concerns when sending data across public networks is confidentiality. Although not all data is confidential, any data you exchange with a remote resource using a WAN is potentially available for anyone else to see. Consider all WANs to be hostile and unsecure. Your organization likely controls access to your LANs and has some measure of assurance of how private the LANs are. WANs are different. You don't have control over who accesses them or who can access data traveling across a WAN. You must deploy sufficient controls to protect the privacy of any data in the WAN Domain.

Implementing Proper Security Controls for the WAN Domain

The primary control type you'll use in the WAN Domain for any data is encryption. You have many encryption choices, and the right control depends on how you'll use the data and which component applies the encryption methods. Your application may encrypt your data or another component may encrypt the connection in another domain. You'll learn about different approaches to encryption later in this chapter. Some solutions require multiple layers of controls. You select the best controls that support a few general principles. These are the same principles that apply in the LAN-to-WAN Domain:

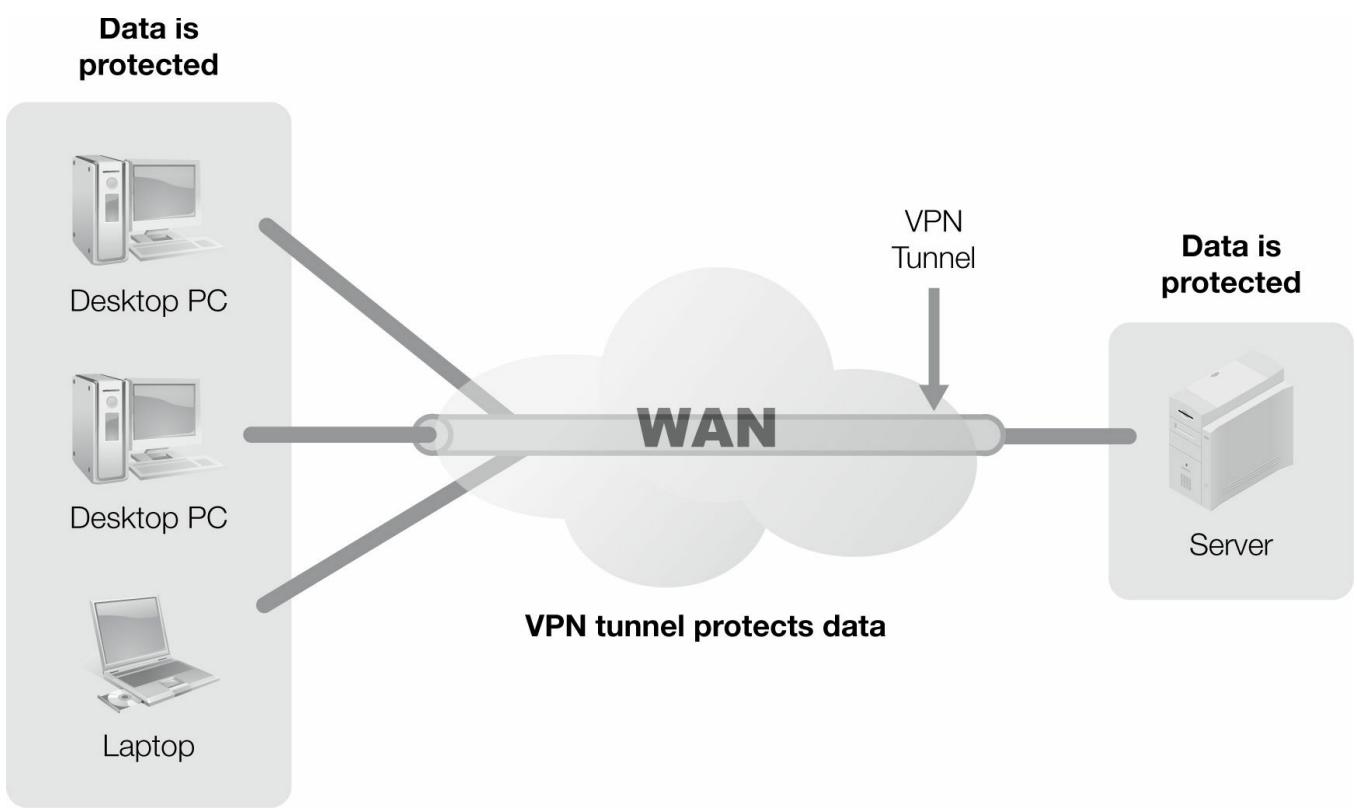


FIGURE 12-3 Protecting WAN traffic using encryption.

- No data in the WAN Domain should ever be transmitted in cleartext.
- When using encryption, select the algorithm based on needs. Don't just select the largest key.
- Assume an attacker can intercept and examine any network messages.

Figure 12-3 shows a simple diagram of how a virtual private network (VPN) tunnel protects encrypted data as it moves across the Internet.

Devices and Components Commonly Found in the WAN Domain

The WAN Domain exists to transport network messages from one node to another. In most cases, the WAN is a network that is owned and managed by some other entity. Your ability to affect the WAN's security is limited or nonexistent. You must ensure that you transmit data across the WAN in a secure fashion using secure protocols and techniques. In this section, you'll learn about the devices and components you'll commonly find in the WAN Domain that support communication, both secure and unsecure. Once you've learned about the devices and components, you'll learn about controls to ensure compliance in the WAN Domain.

WAN Service Providers

Few organizations have the resources to create and manage their own global WANs. The most common approach to deploying applications and functionality across a WAN is to lease network access from a **WAN service provider**. A WAN service provider provides WAN bandwidth to subscribing organizations. The WAN transports traffic among subscriber nodes and subscribers pay for the service. The WAN service provider handles all routing, connection media, and hardware issues within the WAN. All the subscribers do is connect to

the WAN and use it to send and receive traffic.

The three main concerns when selecting a WAN provider are cost, speed, and stability. There are other factors to consider when selecting a WAN, but these three are often the most important. Each type of WAN has its own characteristics and works best in different types of environments.

WAN service providers offer several types of WANs for different budgets and performance requirements. Each type of WAN has its strengths and weaknesses. You need to evaluate each option based on your specific needs to find the best fit for your organization. [Table 12-1](#) lists the main types of WANs available from WAN service providers.

One of the three primary considerations of how well a particular WAN fits your business requirements is stability. An inexpensive WAN that is very fast isn't worth very much if it doesn't stay operational as often as you require. Examine the WAN service provider's **service level agreement (SLA)**. The SLA states a level of guaranteed uptime. In most cases, WAN service providers will provide several levels of service for different subscription amounts.

TABLE 12-1 WAN options.

WAN TYPE	DESCRIPTION	COMMENTS
Dedicated line/leased line	A point-to-point connection between two physical devices	Most secure, but also one of the most expensive; exclusive access to all bandwidth
Circuit switching	A dedicated circuit established between two points for the duration of a conversation	Lower cost, but requires time to establish circuit and circuit switching is slower than the next two options
Packet switching	Messages travel in variable-length packets along point-to-point or point-to multipoint links through WAN switches	Can be substantially faster than circuit switching but media is shared and can suffer congestion
Cell relay	Similar to packet switching but with fixed-length cells	Best for transporting voice and data but overhead can reduce speed
VPN over Internet	A VPN established between two nodes	Very inexpensive but performance and stability depend on your Internet connection

 **NOTE**

Although cost is only one factor when considering a WAN provider, it can be a determining factor.

 **NOTE**

With a dedicated line, or a dedicated circuit, you don't share the bandwidth with anyone else. The entire bandwidth is always available for your use. Because the circuit is permanent, there is no overhead in creating a circuit.

Also pay attention to the cost for WAN service. Some WAN providers offer service for a fixed monthly fee, whereas other products carry a usage charge. Estimate your monthly usage and calculate your costs for each type of service.

Dedicated Lines/Circuits

Your particular WAN needs will direct you toward the best WAN choice. If your primary need for a WAN is to connect a small number of LANs to one another, dedicated lines might be the best choice. A **dedicated line**, also called a dedicated circuit, is a permanent circuit between two endpoints. A single dedicated line works very well when connecting two LANs, campus area networks (CANs), or even metropolitan area networks (MANs). You can connect more than two networks using multiple dedicated lines.

Dedicated lines are fast, secure, and always available. Because no one else shares your dedicated line with you, your organization has exclusive access to the traffic flowing along the line. Of course, the WAN service provider has access to your traffic as well, but no one else should be able to see your traffic. If your budget and connectivity needs support dedicated lines, they can return some of the best performance of all WAN options.

MPLS/VPN WAN or Metro Ethernet

If your requirements include connecting more than three or four locations—for example, connecting multiple branch offices to the headquarters—dedicated lines will likely be too expensive. Another option in such a case is Multiprotocol Label Switching (MPLS) networks supporting a VPN. MPLS works with many WAN technologies and provides very good overall performance using packet-switching and circuit-switching networks. Although MPLS networks are not optimal for high-bandwidth, large-volume network transfers, they work very well in most environments where you need to maintain connections between several other networks.

For high-bandwidth needs within smaller geographic regions, a hybrid of a WAN and a LAN has emerged that fills a particular niche of small WANs. Historically, MANs have been implemented as small-scale WANs using WAN protocols. Technical advances in networking hardware and connection media have enabled the deployment of the well-known Ethernet technology in larger networks. **Ethernet**, a longtime favorite LAN protocol, is inexpensive to deploy and provides substantial bandwidth for the low cost. This hybrid network that uses Ethernet in a MAN is called an **Ethernet MAN** or **metro Ethernet**.

WAN Layer 2/Layer 3 Switches

Most discussions of network protocols include a discussion of the **Open Systems Interconnection (OSI) reference model**. The OSI reference model is a generic description for how computers use multiple layers of protocol rules to communicate across a network. The OSI reference model defines seven different layers of communication rules. You'll also likely encounter another popular reference model, the **Transmission Control Protocol/Internet Protocol (TCP/IP) reference model**, when discussing network protocols. The TCP/IP reference model defines four different layers of communication rules. Both models are useful to describe how protocols work and how to implement them in network communications. [Figure 12-4](#) shows the TCP/IP reference model and the OSI reference model.

You might hear hardware devices or software protocols referred to as Layer 2 devices or Layer 5 protocols. These references generally refer to the OSI reference model layer to describe where the referenced hardware or software operates. In the context of WANs, most WAN protocols operate at OSI Layer 2. MPLS actually operates between Layers 2 and 3 and is sometimes called a Layer 2.5 protocol. Most traditional network switches operate at OSI Layer 2, but newer devices use advanced techniques to provide more sophisticated switching capabilities at OSI Layer 3.

Recall that traditional Layer 2 switches use the Media Access Control (MAC) addresses in each packet to forward the packet to its proper destination. One type of Layer 3 switch extends the concept of a traditional Layer 2 switch by implementing fast Internet Protocol (IP) routing using hardware. Most routing using IP addresses requires software to examine each packet. Software is always slower than hardware and, thus, routing has historically been slower than switching. A Layer 3 switch can greatly speed up routing by using advanced hardware to make the routing decision.

TCP/IP reference model



OSI reference model

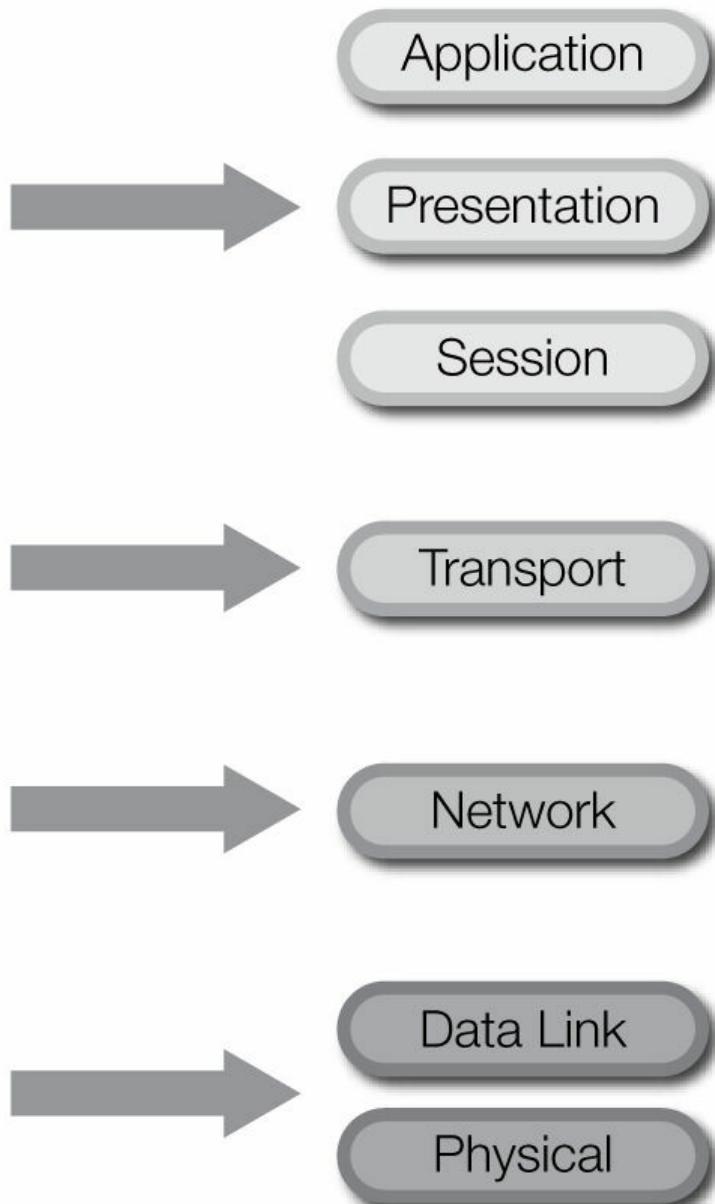


FIGURE 12-4 TCP/IP and OSI reference models.

Layered Protocols in Real Life

The idea of layered protocols sounds complex, but it really reflects what happens in normal human-to-human communication. You use layers and translations in subtle ways every time you talk with a different person. Here's an example that demonstrates the obvious need for multiple layers. Consider how ambassadors communicate in the United Nations. Suppose a U.S. ambassador wants to send a

written note to the ambassadors of China, Russia, and Italy. In this example, protocol requires all written messages be presented in French. Here is how the message travels through the United Nations:

1. The U.S. ambassador writes a message in English, then hands the message to a translator.
The ambassador layer passes the message to the translator layer.
2. The translator translates the message into French, then hands it to an aide to take to the mailroom.
The translator layer passes the message to the aide layer.
3. The aide makes three copies of the message, addresses each copy, and places the messages in the U.S. outbox in the mailroom.
The aide layer duplicates and passes the messages to the mailroom clerk layer.
4. The mailroom clerk picks up the messages from the U.S. outbox and places them in the appropriate inboxes for China, Russia, and Italy.
The mailroom clerk handles the physical transfer.
5. An aide for each country—China, Russia, and Italy—picks up the message and delivers it to the translator.
The aide layer collects a message from the mailroom and passes it to the translator layer.
6. The translator translates the message from French into the country's natural language and gives it to the appropriate ambassador.
The translator layer translates the message and passes it to the ambassador layer.
7. The ambassador for each country reads the message and takes appropriate action.
The ambassador layer reads the message.

Figure 12-5 illustrates the process.

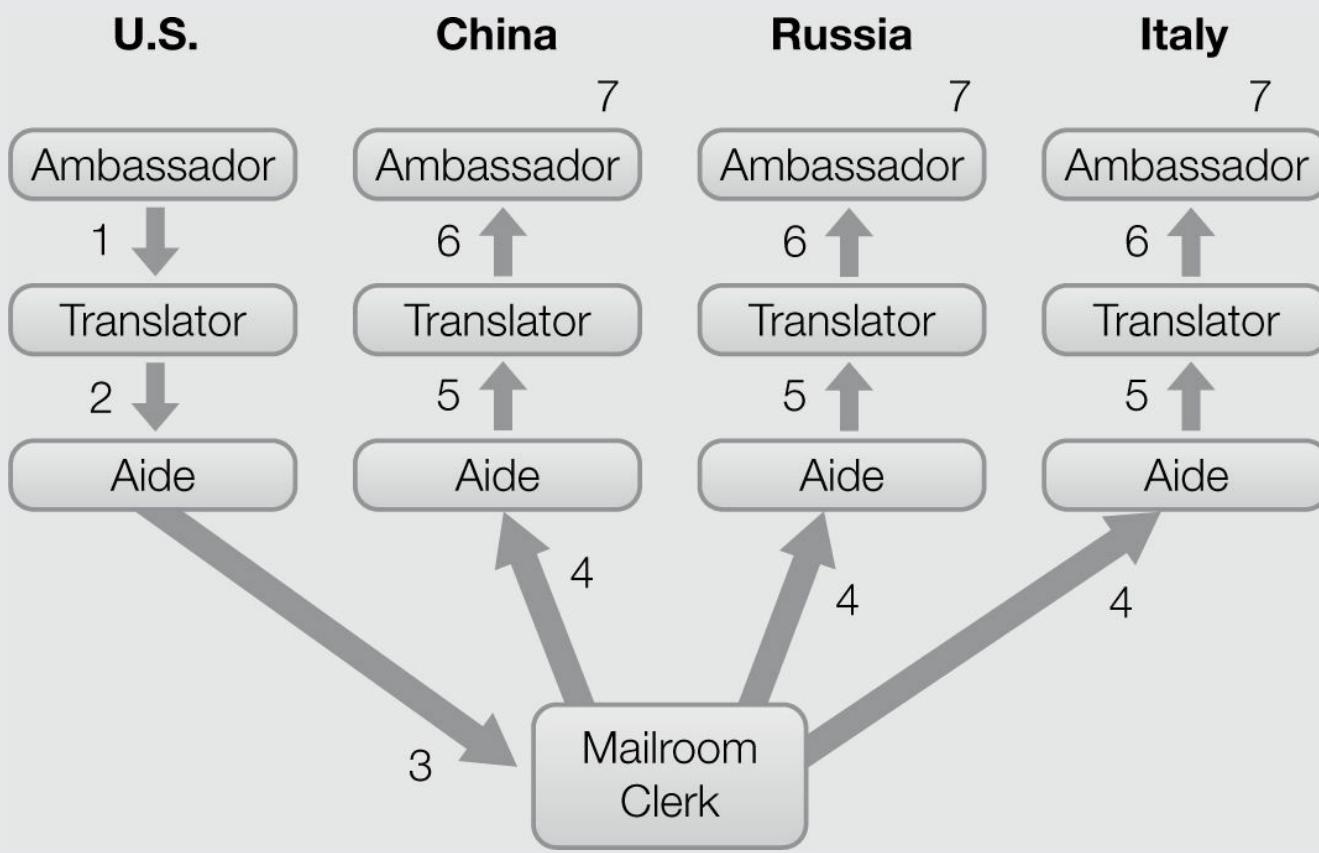


FIGURE 12-5 Message flow in the U.N. example.

WAN Backup and Redundant Links

All components in all domains can fail. If this happens, it's important that each component

have a backup or alternate component to replace it. Your WAN connection is no exception. If your organization relies on a single WAN connection and that connection fails, access to your WAN fails.

Keep in mind the importance of redundant and alternate WAN connections in the LAN-to-WAN Domain. The issue bears repeating here. Remember that your organization's ability to use a WAN to communicate with central resources and functions depends on the availability of your WAN to support the connection. A failure anywhere in the WAN violates your organization's data availability. Make sure you take these steps to protect the availability and security of your data across the WAN Domain:

- Ensure the SLA for each WAN service provider meets or exceeds the required uptime goals for each WAN.
- Establish backup or redundant WAN connections—either multiple connections to the same WAN or multiple connections using different WANs.
- Install backup or redundant connection devices in the WAN Domain to ensure connection hardware failure does not result in a failure to connect to your WAN.

WAN Traffic and Performance Monitoring and Analysis

Monitoring the traffic and performance of your WAN Domain can directly translate into concrete results. WAN usage might cost money, but it always costs time. Anytime you can reduce WAN usage, you are saving time and perhaps money as well. Recall that a secure network is one that provides smooth operation and allows only authorized traffic. Access to your WAN is one of the necessary pieces in a distributed environment. If the WAN is down or unreachable, your distributed applications can't function. Network problems could cause service interruptions and could result in noncompliance. You need to be aware how all parts of your network are working to ensure you are compliant.

Traffic monitoring and analysis for a WAN are nearly identical to the process used with the LAN-to-WAN Domain. The WAN Domain differs from other domains in that you probably don't own or control the hardware or the software in the WAN. Your organization likely pays a subscription fee to connect to another organization's WAN. You generally pay the WAN service provider either by bandwidth usage or a flat fee for a specified bandwidth limit. Because you likely pay for WAN access, proactively managing WAN traffic can reduce your need for additional bandwidth and reduce your WAN costs.

You can implement WAN traffic-monitoring and analysis software and devices in two ways. You can install software or devices on the perimeter of the WAN where you connect to it or rely on your WAN service provider to supply traffic-flow data. You gain far more control monitoring the WAN yourself, but you only have limited capability to affect the WAN's performance. One technique is to send a message to another node on the WAN and have that node echo a response. The first node can analyze the route and duration the message took for the round trip. Comparing sample traffic with baseline data will reveal if the current performance is normal.

Several vendors provide tools to help monitor WAN traffic and optimize your WAN's throughput. Real-time WAN optimization software can analyze current WAN performance and then modify how new traffic is sent across the WAN. These **WAN optimizers** can exclude unnecessary traffic, use compression to maximize bandwidth, cache data, and prioritize traffic to make the best use of your WAN. The result can be a noticeable increase in network speed. In this case, you haven't made the network any faster but you have used the available bandwidth more efficiently and increased your data throughput. [Table 12-2](#) lists some WAN

optimization products.

You can choose from many products to help optimize your WAN usage. Explore the solutions presented here (as well as elsewhere) and select a product that best meets your security goals.

TABLE 12-2 WAN optimization tools.

PRODUCT	WEB SITE
Riverbed SteelCentral	http://www.riverbed.com/products/performance-management-control/
ManageEngine OpManager	http://www.manageengine.com/products/opmanager/router-monitoring.html
BlueCoat WAN Optimization product line	https://www.bluecoat.com/products/mach5
Cisco WAN Optimization	http://www.cisco.com/c/en/us/products/routers/wide-area-application-services/index.html
F5 WAN optimization solutions	http://www.f5.com/solutions/acceleration/wan-optimization/

WAN Configuration and Change Management

As with the LAN and LAN-to-WAN Domains, managing network-configuration settings in the WAN Domain is important. You don't, however, have nearly the control over the WAN network components because most of the actual devices belong to your WAN service provider. Regardless, you still need to proactively manage the components you do control. You can manage the settings of at least these WAN Domain components:

- **WAN access device**—This is the device or computer you use to physically connect to your WAN.
- **WAN account**—Your WAN service provider will provide access for you to configure specific settings to your WAN account. It is important that you create a backup of these settings. Even if your WAN service provider only allows you to manage your account using a Web page, saving screen shots of each configuration page is better than having no record of your settings.
- **WAN optimization device**—Any hardware or software that optimizes WAN traffic belongs to the WAN Domain and is a prime candidate for configuration management.

The strategies and techniques for managing configuration settings and controlling configuration changes should match your activities in the LAN and LAN-to-WAN Domains. As with other domains, managing the configuration settings of your WAN Domain components is an important part of keeping your overall environment compliant and secure.

WAN Management Tools and Systems

Because the WAN service provider bears the responsibility of maintaining the actual WAN, there isn't much left to do to manage components in your WAN Domain. It is important to ensure all the components in the WAN Domain are doing their jobs, but there isn't much you can do to manage the actual WAN. You learned about WAN optimization tools earlier in this chapter. Managing components in the WAN Domain primarily means managing how well

your organization uses the WAN resources. There are three main categories of WAN management tasks:

- Providing the best WAN option for specific traffic
- Caring for WAN Domain components
- Optimizing WAN usage

In this respect, the WAN optimization tools from [Table 12-2](#) are also WAN management tools. Your organization likely has different needs for WANs. As a result, you will likely use different WAN solutions. You may make the decision of which WAN to use in other domains, but the actual access point exists in the WAN Domain. It is important to ensure each WAN access point is configured and optimized to provide the best level of service for your needs.

Mixed WANs

Your organization doesn't have to choose only a single WAN solution. Organizations commonly use multiple WAN solutions to best meet their needs. For example, you might select dedicated lines to connect your headquarters building to your R&D facility, a packet-switching network to connect branch offices that need only data services, and a circuit-switching network for branches that need voice and data services. You could also use a metro Ethernet network for the branch office that is located in the same city as your headquarters building. Such a solution with multiple WANs can give you the best performance for your distributed enterprise needs.

Access Rights and Access Controls in the WAN Domain

Because there are limited components in the WAN Domain, there are also limited opportunities to enforce access control for the domain. There are essentially two places to control access to the WAN. First, you can deploy controls to limit access to the WAN access device. Device and user authentication and authorization controls should limit which users can access the WAN access point. The second way to control WAN access is in the access device itself. The WAN access point has the ability to enforce access controls. In this way, the WAN access device controls which users can get through the device and onto the WAN.

WAN access devices and WAN optimization devices both contain the ability to selectively grant access to the WAN. Although the WAN access device generally operates like a firewall or gateway, WAN optimization devices can make more sophisticated decisions about WAN access. Granting access may include decisions regarding time- or bandwidth-sensitive rights. Some users might be granted WAN access only during slow periods, while other users might get access on demand. You have the ability to grant or deny WAN access based on your security and functional needs.

Implementing more complex controls means you should spend more time testing the controls under different circumstances. If you implement load-based controls using WAN optimization, ensure you test the controls under different network loads, either real or simulated. Use auditing to create logging entries for repeated access denials to ensure your controls aren't hampering your users' ability to do their jobs. As always, avoid auditing too many events. Only audit the ones you'll need to analyze your WAN's ongoing performance.

Maximizing C-I-A

The main goal in all domains is to deploy and maintain controls that support all of the C-I-A properties of security for your data. The WAN Domain contains several components that play critical roles in providing secure access to your organization's data. Maintaining that security requires diligence and the right controls.

WAN Service Availability SLAs

Each WAN service contract includes specific promises of stated levels of service called service level agreements (SLAs). SLAs state what your WAN service provider promises to deliver in terms of various types of services. Most WAN service provider SLAs address the availability property of data security. You should subscribe to a WAN service that guarantees the level of availability your organization requires to conduct business.

Availability SLA terms depend on the type of service you purchase. Most WAN service providers offer customers a choice of service guarantees for different costs to meet different customers' needs. [Table 12-3](#) shows a sample list of availability service choices. Note that the levels of service differ based on the reliability or recovery options selected.

The level of availability you choose will dictate the cost and hardware requirements for your WAN service. Examine the impact of expected or scheduled annual downtime and select the level of service that fits your organization.

WAN Recovery and Restoration SLAs

Most WAN service provider SLAs also include provisions for recovering from major interruptions due to hardware or carrier failure. Each SLA should contain a commitment for the maximum amount of time it should take to restore your organization's WAN service after a failure. The **time to recover (TTR)**, or time to repair, commitment states the acceptable amount of time that is allowed to repair or replace failed components. For global networks, WAN service providers often employ the services of local technicians to decrease response time. The WAN service provider would have its own SLAs with its subcontractors.

As with the availability SLA, you should select a recovery SLA that meets your organizational goals for data availability. Review your own plans to ensure that when your WAN service provider restores its service, you are ready to connect and use the WAN to continue your business operations.

TABLE 12-3 Availability service choices.

SERVICE	AVAILABILITY	COMMENT
Dual routers/dual circuits	100%	Redundant hardware and connections provide uninterrupted service.
Single router with backup	99.95%	Backup hardware can replace the primary router with very little downtime. The estimated annual downtime is 4.4 hours.
Single router	99.5%	A single router is a single point of failure—and you must replace failed hardware. The estimated annual downtime is 43.8 hours.

WAN Traffic Encryption/VPNs

SLAs define levels of service that protect the availability property of data. Additional concerns when sending data across any WAN include integrity and confidentiality. The main type of control you can use to ensure the integrity and confidentiality of your data is encryption. One

of the more common types of encryption in use in the WAN Domain is encrypted traffic over a VPN.

A VPN is a persistent connection between two endpoints, commonly created over a WAN. Although not limited to WANs, VPNs make it easy to establish what appears to be a dedicated connection over a shared-access WAN. VPNs work well in creating persistent connections, also called tunnels, over the Internet or other types of WANs. Many VPNs also encrypt the traffic in the tunnel, making it an attractive option for WAN traffic that may contain sensitive data. Encrypted VPNs are also called **secure VPNs**. Even though others might be able to see the traffic as it travels through the WAN, no one can read it or change it without being detected because the data is encrypted.

 **NOTE**

VPNs provide secure access to remote users and are particularly pertinent to the Remote Access Domain.

Today's networks often support multiple VPN protocols. Consult your WAN service provider for information on which VPN protocols your WAN supports. Use VPNs anytime you need to ensure integrity and confidentiality when sending data over a WAN. [Table 12-4](#) lists some of the more common VPN protocols in use today.

TABLE 12-4 Common VPN protocols.

PROTOCOL	DESCRIPTION
Layer 2 Tunneling Protocol (L2TP)	This common tunneling protocol defines a connection between two endpoints. You need another protocol, such as Internet Protocol Security (IPSec), to provide encryption services.
Point-to-Point Tunneling Protocol (PPTP)	This Layer 2 protocol defines a tunnel between two endpoints. PPTP is older and generally less secure than L2TP.
Secure Sockets Layer/Transport Layer Security (SSL/TLS)	This common protocol is used to transport encrypted Hypertext Transfer Protocol (HTTP) traffic. It can also be used to create an encrypted tunnel.
Datagram Transport Layer Security (DTLS)	This protocol is used by Cisco hardware to create a generic VPN that works well in most network architectures.
Secure Socket Tunneling Protocol (SSTP)	SSTP works at the Transport Layer to provide a VPN that works with most firewalls.

WAN Service Provider SOC Compliance

For service providers, it's important to instill trust and confidence in their customers. Service organizations have a vested interest in helping their customers understand that adequate controls and processes are in place. The Service Organization Controls (SOC) reports provide such assurance. The Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) issues and maintains these auditing standards.

An SOC report signifies that a service organization has had its control objectives and activities examined by an independent auditing firm. Because so much emphasis is placed on

security and compliance with multiple sources of requirements, service providers must demonstrate that they have adequate controls in place to securely handle their customers' data. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act make SOC audit reports even more important to the process of reporting on the effectiveness of internal control over financial reporting.

SOC reports take the form of three different engagements, which product three different reports. The following are the three types of engagements and associated SOC reports:

- **SOC 1, "Report on Controls at a Service Organization Relevant to User Entities Internal Controls over Financial Reporting"**—These reports are based on "Statement on Standards for Attestation Engagements (SSAE) No. 16." Simply known as SSAE 16, it has replaced what was commonly known as "Statement on Auditing Standards (SAS) No. 70," or SAS 70. This report is intended to provide assurance to organizations (user entities) that rely on the service provider. These reports are used by auditors of the user entities with regard to performing financial audits. There are two types of SOC 1 reports. These include type 1 and type 2. A type 1 report includes the auditor's assessment of the fairness of the description of the service organization's system as of a specific date. A type 2 report is similar but also reports on the effectiveness of the controls through a specific period.
- **SOC 2, "Report on Controls at Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy"**—An SOC 2 report was specifically created to address the wide and growing use of technology and cloud-based providers. As the name of the report implies, the SOC 2 considers the security, availability, integrity, and confidentiality of the service organization's system and data. As with SOC 1, there are two types of SOC 2 reports: type 1 and type 2. A type 1 report provides management's description of the organization's systems and suitability of controls. A type 2 report does the same, but also includes management's assessment of the effectiveness of the controls.
- **SOC 3, "Trust Services Report for Service Organizations"**—An SOC 3 report is similar to an SOC 2 but may be more appropriate for a service provider when the provider's customers don't have the need or knowledge to use the details provided by SOC 2. Unlike SOC 1 or SOC 2 reports, which are intended for specific audiences or restricted, SOC 3 reports can be freely distributed.

An SOC compliance audit demonstrates that a WAN service provider stands behind its security controls and has confidence in its ability to protect customer data. You should insist on doing business only with WAN service providers who can show evidence of the appropriate SOC reports.

Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines

Compliance in the WAN Domain depends on implementing the best controls you can and on ensuring your WAN service provider's controls are compliant as well. As with other domains, you should explore alternative controls for each security goal. You must ensure the correct controls are in place to balance each of the three C-I-A security properties.

As you analyze controls in the WAN Domain to meet compliance requirements, ensure each control satisfies your security policy. If a control does not support any part of your

security policy, you should question its value to your organization. Although different legislation, regulations, and vendor standards have different requirements, [Table 12-5](#) lists the types of controls for which you'll likely need to ensure compliance in your WAN Domain.

Implementing multiple types of controls decreases the likelihood that an attack will be successful and makes your WAN Domain more secure.

Best Practices for WAN Domain Compliance

The WAN Domain allows multiple locations to establish network connections without having to manage the physical networks yourself. Because this domain connects your environment to an untrusted WAN, you must ensure the controls protect your internal resources. Solid planning, along with aggressive management, can provide both easy access across an untrusted WAN and the ability to maintain your data's security.

The following best practices represent what many organizations have learned. Plan well and you can enjoy a functional WAN Domain that makes internal information and resources available for use to WAN users. Here are general best practices for securing your WAN Domain:

- Map your proposed WAN architecture, including redundant and backup hardware and connections, before establishing WAN service. Use one of the several available network-mapping software products to make the process easier. Update the network map anytime you make physical changes to your network.
- Establish multiple WAN connections to avoid any single points of failure. Use fault-tolerant hardware that can maintain WAN connectivity if the primary connection or devices fail.
- Use load-balancing techniques on the multiple WAN connections to use the bandwidth of both connections.

TABLE 12-5 Common compliance controls in the WAN Domain.

Type of Control	Component	Description
Preventive	Enforce privacy through encryption	Deny any unencrypted traffic the ability to travel to the WAN.
	Optimize WAN throughput	Use a WAN optimizer to identify and deny unnecessary WAN traffic.
	Assurance of WAN service provider security	Insist that all WAN service providers provide evidence of the appropriate SOC report.
	Assurance of WAN availability	Establish WAN service that provides SLAs that meet or exceed your organization's uptime and recovery requirements.
	User-based access controls for WAN resources	Restrict access to the WAN to reduce traffic and resource exposure.
Detective	Configuration change control	Limit changes to all network device configuration settings and filtering rules. Require approval for all changes before deploying them.
	Performance monitoring	Frequently sample WAN traffic flow metrics and alert for any unusual activity.
	Traffic analysis	Examine traffic for known attack signatures and to ensure data is encrypted.

	Configuration settings monitoring	Compare WAN device configuration settings with stored baselines to detect any unauthorized changes.
	Penetration testing	Conduct periodic penetration tests to identify security control weaknesses.
Corrective	WAN component patching	Keep WAN devices and applications patched to the latest available level.
	Attack intervention	Automatically modify filtering rules to deny traffic from sources generating known attack signature packets.
	Business continuity plan (BCP) and disaster recovery plan (DRP)	Develop and maintain plans to survive and continue operations in the face of small or large disruptions. Coordinate your BCP and DRP with your WAN service provider's SLAs.

- Develop a backup and recovery plan for each component in the WAN Domain. Include recovery plans for damaged or destroyed connection media. Don't forget to include configuration settings for network devices in your backup and recovery plans.
- Implement frequent update procedures for all operating systems, applications, and network device software and firmware in the WAN Domain.
- Monitor WAN traffic for performance and packets for suspicious content.
- Carefully control any configuration setting changes or physical changes to domain nodes. Update your network map after any changes.
- Use automated tools whenever possible to map, configure, monitor, and manage the WAN Domain.
- Use WAN optimization devices or software to maximize WAN utilization.

These best practices give you a brief overview of the issues you'll need to consider when implementing WAN access. Consider each of the best practices and add your own that will make your organization safer when transporting data across a WAN.



CHAPTER SUMMARY

The WAN Domain allows your users to connect to your resources and applications through a WAN from anywhere the WAN reaches. Opening your environment up to a WAN also opens new possibilities for attacks from WAN users. Connecting to a WAN offers many advantages and pitfalls. Learn about the components in the WAN Domain and how to secure them. Through solid planning, you can empower your users with the flexibility and functionality of WAN access while minimizing the security issues.



KEY CONCEPTS AND TERMS

Dedicated line
Ethernet
Ethernet MAN
Metro Ethernet
Open Systems Interconnection (OSI) reference model

Secure VPNs

Service level agreement (SLA)

Transmission Control Protocol/Internet Protocol (TCP/IP)

Time to recover (TTR)

WAN optimizers

WAN service provider



CHAPTER 12 ASSESSMENT

- 1.** The WAN Domain commonly contains a DMZ.
 - A. True
 - B. False
- 2.** One of the most important concerns when sending data across a WAN is confidentiality.
 - A. True
 - B. False
- 3.** Which of the following is the primary type of control employed in the WAN Domain?
 - A. Firewalls
 - B. Encryption
 - C. Hashing
 - D. Compression
- 4.** Who writes SLAs?
 - A. Subscribing organization
 - B. Telecom company
 - C. WAN service provider
 - D. SOC
- 5.** Which type of WAN generally has the highest speed and is most secure?
 - A. Dedicated line
 - B. Circuit switching
 - C. Packet switching
 - D. MPLS network
- 6.** The _____ contains the guaranteed availability for your WAN connection.
- 7.** Which WAN technology is a cost-effective solution for connecting multiple locations?
 - A. MPLS
 - B. ISDN
 - C. MAN
 - D. L2TP
- 8.** Most WAN protocols operate at which level in the OSI reference model?
 - A. 7
 - B. 3
 - C. 2
 - D. 1
- 9.** A(n) _____ can exclude unnecessary traffic from the WAN.
- 10.** WAN subscription cost tends to decrease as availability increases.
 - A. True
 - B. False

- 11.** By definition, VPN traffic is encrypted.
A. True
B. False
- 12.** Which of the following is an internal control report for the services provided by a service provider?
A. SLA
B. WAN
C. SOC
D. MPLS
- 13.** A _____ makes it easy to establish what appears to be a dedicated connection over a WAN.
- 14.** Which of the following describes a common LAN protocol deployed to a network the size of a city?
A. IPsec MAN
B. Urban Ethernet
C. TCP MAN
D. Metro Ethernet

CHAPTER 13

Compliance Within the Remote Access Domain

O

RGANIZATIONS ARE BECOMING more diverse and dispersed. Many organizations that used to conduct business from a single, central location or a small number of locations are now finding themselves spread out across many areas. Employees work from home and while on the road. Customers and partners need access to information to maintain their business relationships. Many organizations are finding that supporting remote access to their data is a primary requirement for doing business in today's global economic environment. Both applications and users are increasingly demanding to access data from remote locations, often using untrusted wide area networks (WANs). Extending trust to remote users requires more planning and effort but provides the basis for keeping data secure regardless of how far it travels.

Securing data as it travels from your protected internal network across an untrusted WAN to remote users depends on the ability to trust in the identity those users provide. Not only do you establish trust when you establish a connection, you also establish trust throughout the conversation. You need to trust the user or entity on the other end of a connection during each data exchange. The purpose of the Remote Access Domain is to provide mechanisms to establish and maintain trust between remote users and components within other domains in your organization. In this chapter, you'll learn about the Remote Access Domain, the components commonly found in the domain, and techniques to keep the domain secure and compliant.

Chapter 13 Topics

This chapter covers the following topics and concepts:

- How compliance law requirements relate to business drivers
- Which devices and components are commonly found in the Remote Access Domain
- What remote access and virtual private network (VPN) tunnel monitoring are
- What remote access traffic and performance monitoring and analysis are
- What remote access configuration and change management are
- Which remote access management tools and systems are commonly used
- What access rights and access controls in the Remote Access Domain are
- What Remote Access Domain configuration validation is
- How to ensure adherence to documented IT security policies, standards, procedures, and guidelines
- What best practices for Remote Access Domain compliance are

Chapter 13 Goals

When you complete this chapter, you will be able to:

- Identify compliance law requirements and business drivers
- Compare how devices and components found in the Remote Access Domain contribute to compliance
- Describe methods of ensuring compliance in the Remote Access Domain
- Summarize best practices for Remote Access Domain compliance

Compliance Law Requirements and Business Drivers

Empowering users from many locations to use resources that are not located near them makes economic sense. In most cases, shared resources are less costly than duplicated resources. Of course, sharing resources only makes sense if you can do it securely in a way that supports your business functions. Providing effective and secure access for remote users and resources is the primary focus of the Remote Access Domain.

This domain contains the components that can bring your distributed environment together and make its resources available to remote users. When your organization provides this level of service, you are enabling remote users to operate more effectively and efficiently without requiring them to physically be at your main location. This capability is a benefit to users who are geographically separated from your physical resources either permanently or temporarily. Your users can do their jobs from more locations if they can access your resources remotely. The Remote Access Domain provides the access path for your remote users. [Figure 13-1](#) shows the Remote Access Domain in the context of the seven domains in the IT infrastructure.

Take necessary steps to secure your data in all seven domains of the IT infrastructure. Distributing your data far from its secure storage locations exposes it to more threats of attack. You'll likely need to show compliance with one or more requirements that directly address sensitive data sent to remote users. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires controls to protect the privacy of medical data. The Payment Card Industry (PCI) requires credit card privacy controls. Many states require privacy controls on any personally identifiable data. These are only a few of the requirements you'll need to satisfy when supporting remote users. Your security policy should include all the necessary elements to meet compliance requirements and support efficient and cost-effective operation. Making sure you have the proper controls in place to secure the Remote Access Domain is one important part of an overall plan for data security.

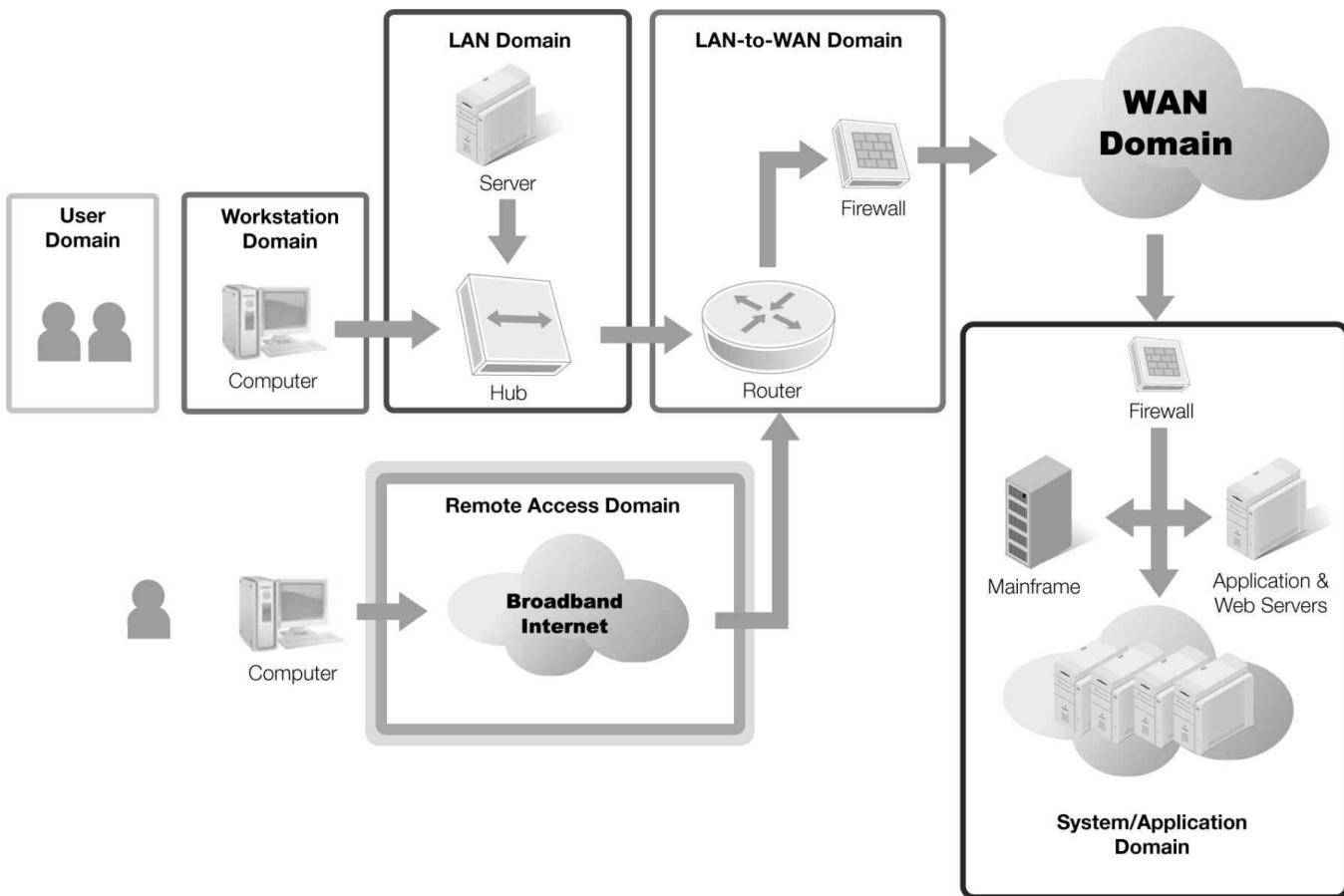


FIGURE 13-1 The Remote Access Domain within the seven domains of a typical IT infrastructure.

Protecting Data Privacy

The primary security concern for remote access is data privacy. Although availability is important, confidentiality and integrity get far more attention in compliance requirements. The most important consideration when allowing remote users to access data is ensuring that private data remains private. Ensuring data privacy essentially means allowing only authorized users to view or modify data. Because remote users commonly use public WANs to access data and applications, keeping sensitive data away from unauthorized users is difficult, if not impossible.

Your organization does not control access to your data on the WAN. The WAN service provider is responsible for controlling access to the traffic it transports. Although you should establish a level of trust with your WAN service provider, you can't enjoy the same level of privacy assurance as you do for data inside your own networks. However, you still must protect the privacy of your data even on the WAN. The specific controls you use are not important. The important goal is to ensure that the privacy of your data does not suffer when it is transmitted to remote users.

Implementing Proper Security Controls for the Remote Access Domain

The most common control for protecting data privacy in untrusted environments is encryption. Recall that encryption is the process of converting readable cleartext to unreadable ciphertext, which can be decrypted only by authorized users. Encrypted data ensures that only users who possess the decryption key can properly decrypt a message. When you provide decryption keys only to authorized users, you protect data from being accessed by unauthorized users.

You must encrypt sensitive data before sending it to a remote user or location to ensure compliance with all appropriate requirements. Technically, you can send data that is not considered sensitive in cleartext. However, classifying data at run time is time consuming and increases the likelihood of missing sensitive data and accidentally sending it in the clear, or unencrypted. It is generally easier and more consistent to encrypt all data transferred in a session. Although you can use a variety of methods to decide what data to encrypt, there are three main strategies for encrypting data to send to remote users:

FYI

Another popular and sometimes preferred alternative to encryption is **tokenization**. Rather than encrypting data, tokenization simply substitutes a randomly generated value for the data. Theoretically, an encrypted value can be mathematically reversed. A token must be mapped back to its original value through a lookup, however. A token by itself cannot be mathematically reversed.

- **Application data encryption**—With this strategy, the application determines what data should be encrypted and encrypts it. The client application on the remote side decrypts the data and presents it to the user. This method of encryption requires substantial effort and overhead but can prevent the encryption of data that does not need it.
- **Application connection encryption**—With this strategy, the application requires clients use secure connections when exchanging data that might be sensitive. An example is the payment screen of an e-commerce application. Although your application may allow customers to shop using unencrypted connections with **Hypertext Transfer Protocol (HTTP)** (an Application Layer protocol most commonly associated with the Web), payment process requires a secure connection with **Hypertext Transfer Protocol Secure (HTTPS)** (a secure version of HTTP). The application validates the connection type, not the actual data. This strategy requires less application interaction than application data encryption and still offers assurance of data privacy. One drawback is the reliance on the connection encryption strength to ensure data privacy. If the connection is not configured well, your data could be at risk.
- **System connection encryption**—This strategy does not require any application intervention or changes at all. The connection with the remote user handles the encryption. The most common way to implement system connection encryption is by setting up a secure virtual private network (VPN). A secure VPN encrypts all traffic on the connection. The system encrypts the data before placing it on the VPN at the endpoint and it is decrypted after it is removed from the remote endpoint. VPNs are useful because they allow any type of application to transfer data across an untrusted network without sacrificing data privacy.

Your budget and the operating systems you support will have an impact on which encryption strategy you select. Each strategy has many choices, each with benefits and challenges. Choose the best option to fit your needs. One of the most popular options to ensure data privacy for remote users is the VPN. Examine the VPN choices available for your environment and select one that meets your security needs.

Although the most common security control in the Remote Access Domain is encryption, don't forget the controls on remote users and the computers they use to access your network from a remote location. Remote users must adhere to your remote access acceptable use

policy (AUP). Encryption can help protect your sensitive data, but a user who isn't careful or a poorly secured laptop can leave the data vulnerable. You'll learn more about the vulnerabilities associated with each Remote Access Domain component in the next section. Make sure you protect all components with the best controls.

Devices and Components Commonly Found in the Remote Access Domain

The Remote Access Domain provides access to remote users and remote resources. It exists, in part, to provide a secure way to exchange data with remote components without sacrificing data privacy. This domain consists of several components that work together with your WAN to ensure that your data is private and your environment is compliant. [Figure 13-2](#) shows the devices and components commonly found in the Remote Access Domain.

Remote Users

The first component of the Remote Access Domain is the remote user. A remote user is a person who uses a WAN to connect to and access resources or applications from a remote location. The first remote users used dial-up connections to access computers and networks remotely. Personnel who traveled often needed to access data from the organization's central database when they were away from the office. This example is a classic case for remote access. The classic solution to this need was to provide a modem or bank of modems attached to the internal network. Users could dial in and access resources just like local users. The growth of high-speed networks and the Internet have changed the connection methods but not the basic requirements and problems.

Remote users pose several problems for data privacy. Those problems that are most common with remote users are as follows:

- **Remote users connect to an organization's resources using untrusted networks**—

Whether you use the Internet or some other WAN, your network traffic flows across someone else's networks and may be intercepted along the way. If there is a packet sniffer on the WAN, you won't know others are examining your traffic.

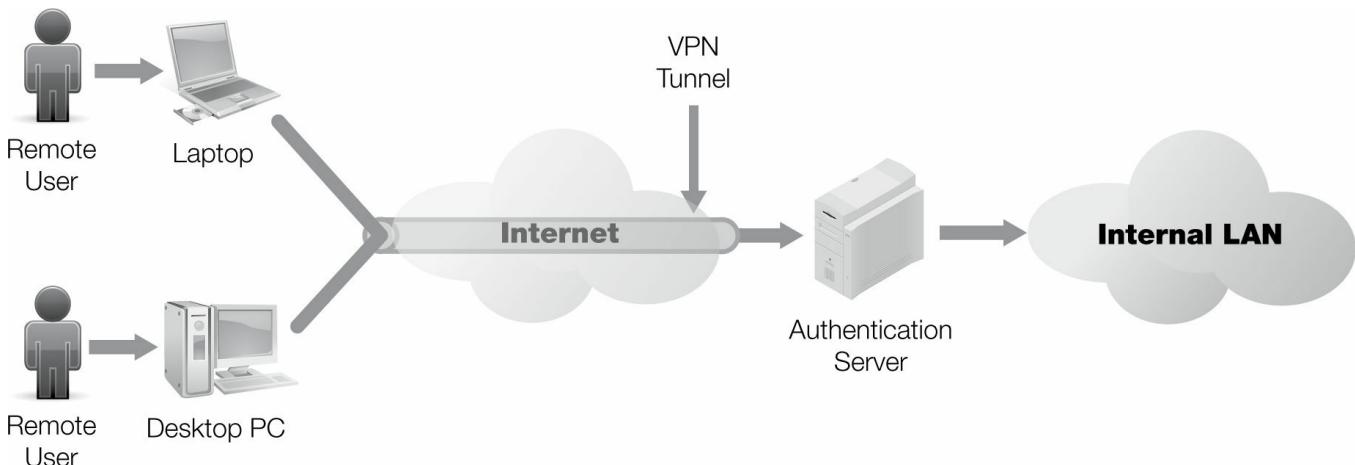


FIGURE 13-2 Devices and components commonly found in the Remote Access Domain.

- **Remote users often use public computers or terminals**—Many travelers use business center computers in hotels to access the Internet and other resources. Users leave

traces of their activities on computers used to access networks. It is possible for users to leave traces of sensitive data after accessing it from a remote location.

- **Remote users can be sloppy**—You must have a strong remote access AUP in place that sets standards for how remote users handle data. Remote access introduces more risk because the data is transferred away from the protection of your organization’s internal controls. Ensure you deploy controls that protect your data all the way to a remote user’s computer—and once it is there.

Remote user access should require a higher standard of care than local user access. Local users enjoy the additional protection of the local environment and its security controls to protect data. Remote users do not have these additional layers of protection. You must ensure that your users agree to comply with your remote access AUP and that you have sufficient controls in place to protect the security of your data even in remote locations.

Remote Workstations or Laptops

Remote users are really just normal users who access resources and applications from a remote location. They use workstations or laptops to establish the connection to the desired resources. In short, the remote user logs on to a computer. The computer accesses a WAN and uses it to establish a connection with other resources. The computer, laptop, or other device becomes the remote device. Remote devices aren’t special devices—they just have the ability to connect to a WAN and establish a connection to some other resource. In fact, more and more tablets and smartphones are capable of acting as remote devices.

FYI

Be careful when allowing devices to act as remote access devices. Smartphones and tablets can cause problems. Many of these devices are not as secure as they might seem. Although most of today’s smart devices that can support VPNs do so well, local data protection support is often lacking. Smaller and more compact devices are ultraportable and easy to misplace. Many of these devices have poor default controls for protecting the data at rest. Initially, many organizations were quick to restrict the use of such devices. That has become less feasible, however. Fortunately, various controls and mobile-device management companies provide solutions to help mitigate the risks.

Remote devices need two main capabilities to handle remote connections in a secure manner:

- **Remote devices must be able to handle encryption**—The most common type of encryption used in remote access is the secure VPN. As long as your device supports the VPN you’ve chosen for remote access and can establish a secure connection, the device passes the first test.
- **Remote devices must be able to protect stored data**—Even when using a VPN, the data gets decrypted when it arrives at the remote device. If your remote device can’t ensure data privacy through its own controls, it should not be allowed to retrieve or process your confidential data.

As computers and other devices mature, it is common to see VPN support and local data privacy protection as standard features. You can use operating system encryption or third-party utilities to encrypt data. Either way, most of today’s computers with recent operating systems already contain the ability to act as secure remote access devices.

Remote Access Controls and Tools

Enabling remote access requires the cooperation of both the remote devices and the remote server. Because remote access depends on one endpoint at the remote location and another endpoint in your local environment, the Remote Access Domain actually spans several domains. By definition, Remote Access Domain components use the WAN Domain to communicate. The Remote Access Domain server components generally reside in the LAN-to-WAN Domain environment even though they still belong to the Remote Access Domain.

When a remote user wants to access the organization's internal network, the remote device requests a connection from the remote access server. The remote access server queries the remote device for identification and authentication credentials. If the identity authenticates, the remote access server grants a connection and rights based on stored authorization information.

The basic steps of the remote connection process don't really differ much from a local logon process. The main difference is that the three basic steps are handled by the remote access server. Once a remote user successfully connects, the user can access resources like any other user. The three basic steps required to establish a remote connection are as follows:

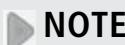
- 1. Identification**—The remote user provides a user ID or user name.
- 2. Authentication**—The remote access server prompts the remote user for authentication credentials. These credentials can be a password, a personal identification number (PIN), a smart card, or data from a biometric reading. The remote access server looks up the stored authentication information for the user. If the authentication credentials provided by the user match the stored credentials, the user is authenticated.
- 3. Authorization**—Depending on the type of remote access server, the authorization information may be stored with the authentication information or in a separate location. In either case, the remote access server looks up the authorization information for the authenticated user and assigns rights and privileges based on the remote user's security settings.

Authentication Servers

The process in the previous section describes how the authentication process works for remote users. There are many ways to authenticate remote users, but three main approaches are used most often. The first two, RADIUS and TACACS+, rely on centralized authentication databases and servers to handle all remote users. Either of these approaches works well when there is a large number of remote users or you need to manage remote users in a central location. You'll learn about the third method, VPNs, in the next section.

RADIUS

Remote Authentication Dial In User Service (RADIUS) is a network protocol that supports remote connections by centralizing the management tasks for authentication, authorization, and accounting for computers to connect and access a network. RADIUS is a popular protocol that many network software and devices support and is often used by Internet service providers (ISPs) and large enterprises to manage access to their networks.



NOTE

The Application Layer is Layer 7 in the Open Systems Interconnection (OSI) reference model,

and Layer 4 in the Transmission Control Protocol/Internet Protocol (TCP/IP) reference model.

RADIUS is a client/server protocol that runs in the Application Layer and uses **User Datagram Protocol (UDP)** to transport authentication and control information. UDP is a core protocol of the Internet Protocol suite. It is a connectionless protocol, which provides no guarantee of delivery. Servers with RADIUS support that control access for remote users and devices communicate with the RADIUS server to authenticate devices and users before granting access. In addition to just granting access and authorizing actions, RADIUS records usage of network services for accounting purposes.

TACACS +

Terminal Access Controller Access-Control System Plus (TACACS+) is another network protocol that was developed by Cisco. TACACS+ has roots back to an earlier protocol, TACACS, but is entirely different. TACACS+ provides access control for remote networked computing devices using one or more centralized servers. TACACS + is similar to RADIUS in that it provides authentication, authorization, and accounting services, but TACACS + separates the authentication and authorization information. TACACS + also uses the Transmission Control Protocol (TCP) for more reliability.

One difference between RADIUS and TACACS + is of interest in a discussion of security. RADIUS only encrypts the password when sending an access request packet to the server. TACACS + encrypts the entire packet. That makes it a little harder to sniff data from a TACACS + packet.

VPNs and Encryption

VPNs are one of the most popular methods to establish remote connections. A VPN appears to your software as a regular network connection. It is actually a virtual connection, also called a *tunnel*, that uses a regular WAN connection of many hops but looks like a direct connection to your software. Most VPNs offer the option to encrypt traffic using different modes to meet different needs.

The concept of **tunneling** is central to most VPNs. Tunneling allows applications to use any protocol to communicate with servers and services without having to worry about addressing or privacy concerns. Applications can even use protocols that aren't compatible with your WAN. Here's how tunneling works:

1. Your application sends a message to a remote address using its Application Layer protocol.
2. The target address your application used directs the message to the tunnel interface. The tunnel interface places each of the packets from the application layer inside another packet using an **encapsulating protocol**. This encapsulating protocol handles tunnel addressing and encryption issues.
3. The tunnel packet interface passes the packets to the layers that handle the WAN interface for physical transfer.
4. On the receiving end, the packets go from the WAN to the remote tunnel interface. There, the packets are decrypted and assembled back into the Application Layer packets and then passed up to the remote Application Layer.

This arrangement provides excellent flexibility and security. Depending on your operating system and VPN solution, you can choose from among several encapsulating protocols.

These include the following:

- **Generic Routing Encapsulation (GRE)**—This tunneling protocol was developed by Cisco Systems as an encapsulating protocol that can transport a variety of other protocols inside IP tunnels.
- **Internet Protocol Security (IPSec)**—This protocol suite was designed to secure IP traffic using authentication and encryption for each packet.
- **Layer 2 Forwarding (L2F)**—This tunneling protocol was developed by Cisco Systems to establish VPNs over the Internet. L2F does not provide encryption—it relies on other protocols for encryption.
- **Point-to-Point Tunneling Protocol (PPTP)**—This protocol is used to implement VPNs using a control channel over TCP and a GRE tunnel for data. PPTP does not provide encryption.
- **Layer 2 Tunneling Protocol (L2TP)**—This tunneling protocol is used to implement a VPN. L2TP is a newer protocol that traces its ancestry to L2F and PPTP. Like its predecessors, L2TP does not provide encryption itself.

technical TIP

Most people associate VPNs with encrypted traffic. Although VPNs are used to encrypt all the traffic transported through the VPN tunnel, encryption is an option and not a part of the VPN itself. The “private” part of VPN really refers to private addressing, not data privacy.

The VPN you select depends on several factors. Some VPN solutions are vendor specific and rely on one type of hardware. Other types of VPNs are operating system specific. For example, the **Secure Socket Tunneling Protocol (SSTP)** is available only for the Windows operating system. SSTP is Microsoft’s attempt to provide a solution that works on any networking hardware. SSTP uses Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer (SSL), to transport traffic. Using SSL or TLS removes many of the firewall and network address translation (NAT) issues some other protocols encounter. Once you have assessed your needs and environmental restrictions, select the VPN solution that best fits your needs for functionality, security, and maintainability.

Internet Service Provider WAN Connections

One of the more common ways to establish remote connections is using the Internet. Because it is easy to establish Internet connections and the access points are numerous, it makes sense to at least consider it for your remote connections needs. Historically, there have been several issues that must be resolved to use the Internet as a remote access WAN:

- **Both sides of the connection must use the same WAN**—When using the Internet as the WAN, all each side must do is establish an Internet connection. The LAN-to-WAN Domain already ensures your internal networks are connected to your WAN. All that is left is for the remote node to connect.
- **Encryption is an absolute necessity**—This is because the Internet is a public use network. VPNs work well to transport data securely over the Internet.
- **Reliable access must be available for remote nodes**—Internet access is becoming easier to find than ever before. Many Wi-Fi hotspots exist to enable computers and

devices to connect to the Internet.

- **Remote connections must be fast enough to be usable**—This requirement is one that will likely cause the most potential issues. Sometimes, especially in more remote areas, it is difficult to find high-speed Internet access. In such cases, it is important to provide access through low-bandwidth methods to ensure data availability.

Although the Internet might not be the fastest WAN, it is quickly becoming the most cost-effective medium and the easiest to use for remote connections.

Broadband Internet Service Provider WAN Connections

The last point in the previous section regarding Internet access was speed. Historically, most users connected to the Internet by dialing into an ISP modem. Modems are rated at speeds as high as 56 kilobits per second (Kbps), although real transmissions rarely sustain the maximum data rate. Even at the highest rate, interacting with remote resources can be slow. As the volume of data that needs to be exchanged increases, dial-up connections are becoming more and more frustrating for remote users.

The alternatives to dial-up include broadband approaches that substantially increase the network connection speed. **Broadband** refers to the technique of only using a portion of the full bandwidth of a channel. Dial-up connections use **baseband** techniques that require the entire channel's bandwidth. Broadband Internet access is defined as any customer connection that provides service at 256 Kbps or higher. Many ISPs now provide asymmetric digital subscriber line (ADSL), cable, wireless, cellular, and satellite connections that are classified as high-speed, or broadband, Internet service. The proliferation of broadband connections makes using the Internet for remote connections an even more attractive option.

Remote Access and VPN Tunnel Monitoring

Any time you allow remote access to your internal protected local area network (LAN) by remote users, you increase the risk of security violations. It is important that you know who is using the remote access features you've enabled to access your resources. There's a lot you can monitor with respect to remote access but the best place to start is by identifying and validating just who is using remote access. There are at least three activities of interest you should be monitoring:

- **Create VPN connection**—Your VPN server has the ability to track both successful and unsuccessful VPN connection requests. Although auditing all connection requests can result in a large amount of data, it can also provide valuable information on how remote users are accessing your resources. Know who is using your resources, where those people are connecting from, and how they are using your VPN.
- **Remote access connection**—After a remote user establishes a VPN, it is interesting to see what that user is doing with it. You can audit resource connections to see how remote users and resources are using your VPN. You should also audit non-VPN remote connection requests. Unless you're using a non-VPN encryption solution, all non-VPN remote connection requests should be denied.
- **Remote computer logon**—Another interesting piece of information you should audit is any remote logons to your computers or devices. Each operating system contains functions to audit logons. In fact, the operating systems can audit much more than just logons. You should be auditing access to sensitive resources at some level. As with all

auditing activity, don't audit more than you need. Audit log files can become very large.

TABLE 13-1 Remote access and VPN monitoring tools.

PRODUCT	SOURCE
CodePlex Remote Access Monitor (open source)	http://remoteaccessmonitor.codeplex.com/
SoftSea Remote Access Monitor (free)	http://www.softsea.com/review/Remote-Access-Monitor.html
Cisco VPN Monitor	http://www.cisco.com/en/US/products/sw/cscowork/ps2326/products_user_guide_chapter09186a008
SNMP	Not a vendor-specific product

The overall idea is to keep track of who is using your VPNs and what they are doing. For example, suppose your primary VPN is optimized for large volumes of small messages. Your expectation when you enabled the VPN was that users would use it to access your online order management system. VPN and remote access monitoring has shown you that most VPN users are running very large custom reports from your database to analyze data. The VPN is actually transporting large volumes of data for a relatively small number of users. You find that you can change some VPN settings that make it run faster for the way your users are using the VPN. Reports run faster and your data is more available. [Table 13-1](#) lists a few programs that help monitor remote access and VPN usage.

The last entry in [Table 13-1](#) is the **Simple Network Management Protocol (SNMP)**. SNMP is a network protocol used to monitor network devices. Most network devices include SNMP support and can run SNMP agents to report conditions that require attention by another computer or device running network management system software. SNMP uses UDP protocol messages to retrieve information from network devices and for the devices to send updates when conditions you define are met. Although there are many ways to use SNMP, you can configure devices to send an alert to the network manager when remote users connect to your network.

Remote Access Traffic and Performance Monitoring and Analysis

It's important to monitor connections and events related to remote access users to learn about who is accessing your network from remote locations. But to ensure your VPNs are configured to best utilize your VPN bandwidth, it is important to also monitor the traffic flowing along your VPNs. Although you can't monitor the contents of traffic in encrypted VPN tunnels, you can monitor traffic statistics to understand how well your remote users are using VPN bandwidth. You can also detect unusual VPN activity that could indicate malicious activity or excessive use.

technical TIP

You should verify that all traffic flowing along your VPNs is encrypted. It is possible to configure VPN tunnels to transport data without encrypting it first. If you misconfigure your VPN or if an attacker is successful at reconfiguring your VPN, you could be sending data into the WAN unencrypted. Validate that the packets flowing along your VPN are actually encrypted.

NOTE

Monitoring VPN traffic does not replace any other types of network monitoring.

Because both endpoints are within domains in your IT infrastructure, you can monitor decrypted packets when they emerge from the end of the VPN tunnel. It is still important that you monitor WAN traffic to understand how your organization uses your WAN connections. VPN traffic monitoring provides additional information on how individual tunnels are behaving within your overall WAN usage. Excessive WAN usage might indicate a network usage problem. Further investigation using VPN monitoring could reveal that one remote user using a VPN is attempting to launch a denial of service (DoS) attack on your organization. In this case, WAN traffic monitoring will have revealed a high-level problem and VPN traffic monitoring will have revealed the cause of the problem. You need to monitor at both levels to get the whole picture.

You can implement VPN traffic monitoring and analysis using the same methods as LAN and WAN traffic monitoring and analysis. You can install software or devices on the perimeter of the VPN where you establish the endpoint. You can also use any of a wide variety of network management software packages that support SNMP to monitor traffic directly from the network devices that transport VPN traffic. Regardless of the methods you employ, monitoring and analyzing VPN traffic is important to ensure your private data is secure and compliant.

Remote Access Configuration and Change Management

It's important to manage the network configuration settings in the LAN, LAN-to-WAN, and WAN Domains. Likewise, managing the changes to your VPN and remote access configuration is crucial to maintaining a secure environment for remote users and resources. As with devices and computers in other domains, you must control configuration changes to Remote Access Domain components, including the following:

- VPN client software
- Authentication servers
- VPN servers
- Remote access servers
- Network management system servers

The strategies and techniques for managing configuration settings and controlling configuration changes should match your activities in the LAN, LAN-to-WAN, and WAN Domains. As with other domains, managing the configuration settings of your Remote

Access Domain components is an important part of keeping your overall environment compliant and secure.

Remote Access Management, Tools, and Systems

Managing remote access components means ensuring each one fulfills the goals for which it was designed. It also means continually updating your configuration to satisfy new and updated goals. Remote access management covers several related activities, including the following:

- Authorizing users and nodes to connect remotely
- Verifying that privacy settings are in place
- Monitoring VPN performance
- Changing configuration settings to optimize performance
- Changing configuration to support new requirements
- Adding necessary controls to address security issues
- Maintaining components of a current recovery process
- Adding, changing, and removing hardware components as requirements dictate

The specific tools and procedures you use to manage remote access components depend on the operating systems and products you use. Configuring remote access users is similar to configuring local users. In fact, remote access settings are generally just additional configuration settings for regular users. For example, in Microsoft Windows Server, you enable remote desktop connections on the server machine and define authorized users using the Remote page of the System Properties window. Then you can set a Group Policy object for users or groups that define specific settings for remote sessions. [Figure 13-3](#) shows the Start a Program on Connection setting in the Group Policy Management Editor.

In addition to operating system settings, some remote access authentication and authorization products require additional configuration information. Learn what your environment requires to define and configure users and devices for remote access. Most network device vendors have their own management software. The remaining management tasks are similar to tasks in the LAN and LAN-to-WAN Domains. The main focus is on ensuring you configure each network device properly and optimally.

Explore options for VPN monitoring and management software for your operating system and network devices. Software that assists your network administrators will likely simplify the management of your VPNs and make it easier to validate compliance with your stated security goals.

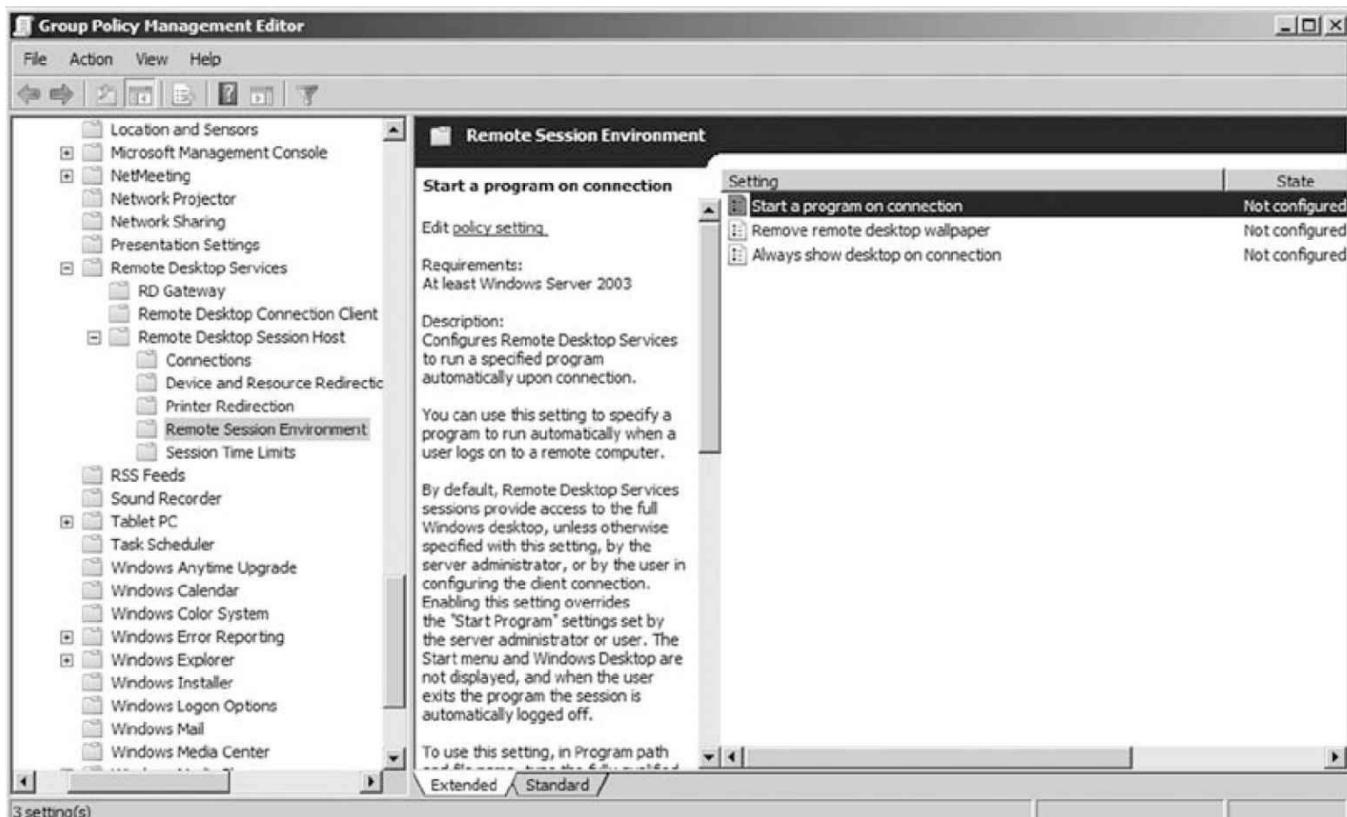


FIGURE 13-3 Windows Group Policy Management Editor.

Access Rights and Access Controls in the Remote Access Domain

The degree to which you grant rights and permissions to remote users depends on your general access model and your operating system. In most cases, remote users accessing your environment via a VPN enjoy the same rights as users on your LAN. The idea behind a VPN is that once it is established, it operates just like a LAN. VPN users are essentially the same as other LAN users. Although it is possible to exclude some users from accessing your network using a VPN at the operating system level, it is generally easier to use the remote access authentication server to define which users can use remote access.



WARNING

Do not include administrative users in a global user list. If you do allow remote administration, you should create administrative accounts specifically defined for remote administration. This practice makes it easier to audit and control remote users with elevated privileges.

The main goal for all networking issues is to keep things simple. Complexity leads to an increased exposure to risk and requires more effort to maintain. Try to keep three lists of users: internal network users, remote access users, and global users. If you don't need to separate most local and remote user rights, then just defining a global user list keeps things simple. After you create the users, you'll need to support remote access. Your operating system provides the ability to define what each user can do through permissions or access control lists (ACLs).

In addition to user rights, your remote access servers can define how you handle remote connections. You should set up VPNs to appear as networks that are separate from your

physical LANs. Defining all VPNs in a specific range of subnets gives you the ability to define filtering or access rules that affect just your VPN connections. Defining rules for VPNs gives you the ability to identify and filter suspicious traffic or any traffic that is not authorized. For example, suppose you want to prohibit remote users from using **Server Message Block (SMB)**, a protocol used to map network resources as shares. You could set a rule in a firewall that sits between your VPN endpoint and your LAN to drop any TCP traffic for the default SMB port, 445. In this way, you prohibit any SMB access from your VPNs.

You can use user rights, permissions, ACLs, and firewall rules to restrict what remote users can do. Document what you'll allow remote users to do and use the appropriate controls to enforce your rules. The more remote users can do, the greater the risk to your data security. Allowing remote users to access your environment can increase your organization's effectiveness at the risk of reducing your overall security. Ensure you have the necessary controls in place to limit what remote users can do and to ensure your data is safe regardless of where it travels.

Remote Access Domain Configuration Validation

Validating compliance in the Remote Access Domain includes validating the controls that satisfy compliance requirements. With respect to the Remote Access Domain, most compliance concerns focus on data privacy. It is important to evaluate all controls to ensure that all three properties of the confidentiality, integrity, and availability (C-I-A) triad are satisfied. There are three main areas of concern in the Remote Access Domain: client-side configuration, server-side configuration, and configuration management verification. Each area focuses on a slightly different component of the Remote Access Domain. Taken together, validating these three areas provides assurance that components in your Remote Access Domain are compliant with the necessary requirements.

VPN Client Definition and Access Controls

Each VPN client stores configuration details to connect to the organization's VPN server. Typically, VPN details include information such as the following:

- Host name or address (primary and backup)
- Logon user name
- Password (optional, dependent on the authentication method)
- Authentication method
- Transport protocol
- Local address options
- Local log settings

Each of the client settings should match the server settings. In some cases, servers support multiple types of clients and will negotiate settings, such as authentication method and transport protocol. It is important that you verify each client's settings to ensure that clients are in compliance with organizational VPN settings standards. One of the easiest ways to verify client settings is to restrict your server settings to deny any connection requests that fall below certain standards. If your clients meet the standards, they can connect. If not, their connections fail.

There are two types of access controls for remote access. The first are the access controls for computers or devices. These access controls define which computers or devices can

establish remote connections. Your authentication servers or VPN servers store computer and device access controls. The location depends on the type of VPN and operating system you are using. The second type of access control is at the user or group level. This type of access control is the same as access control in the User Domain. Once a remote user authenticates and is authorized to access resources, the normal operating system access controls take effect.

TLS VPN Remote Access Via a Web Browser

Most Web development languages and many applications have the ability to require secure connections. For example, you can require that a particular Web page or cookie can only be sent to a client using a secure connection. If the client attempts to render a secure Web page using an unsecure protocol, the page does not render. You would have to use HTTPS to render the page. In other words, you would have to include HTTPS in the address to reach the page.



WARNING

Consult the setup and configuration guide for your Web server. Some Web servers enable all encryption modes by default, including a debugging mode that actually doesn't encrypt traffic. If you leave this option enabled, attackers can trick your Web server into sending private data without using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) with encryption. Unless you're using a VPN, the Web server sends the data in the clear.

To verify compliance with data privacy for remote users, you should enforce the following:

- Require all Web pages that access sensitive data to have secure HTTPS connections or have local host addresses. Local host addresses for Web pages require VPN connections.
- Require all users to be authenticated before accessing any resources or data.
- Allow only VPN nodes to access sensitive data directly.
- Require operating system-and application-specific access controls to define which users can access sensitive data.

Adhering to these rules will ensure your data is safe from unauthorized remote users.

VPN Configuration Management Verification

Recall that the C in FCAPS stands for configuration. You can use tools such as RANCID to help manage VPN configuration settings. Managing all your network devices' configuration settings keeps unauthorized changes from reducing your data's security. RANCID, along with other available tools, can help you create baselines of configuration settings and compare changes over time. You should develop a schedule and process to frequently compare configuration baselines and verify all changes to your network's configuration.

A solid network configuration management process includes managing changes to all configuration settings. A formal process makes it easy to classify any configuration changes as authorized or unauthorized. You just compare baseline differences to your authorized changes list to see which changes occurred that were not authorized. Implementing the FCAPS approach across all your networks will help formalize the process and make your

networks more secure.

Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines

Security doesn't just happen. A secure environment is the result of solid plans and faithful adherence to those plans. If your organization takes the time to plan the best ways to achieve compliance and security assurance, it makes sense to follow those plans. Each component of your plans should address one or more of the basic C-I-A properties of data security. As you select and deploy controls, ensure that each one supports your organization's security policy. Many organizations end up deploying controls that seem good but are not indicated in their policy. Such a situation indicates that either the control is not needed or the policy needs amending. In either case, your controls should be the result of enacting your security policy. Above all else, it is important that your security policy be current and complete. [Table 13-2](#) lists the types of controls you'll likely need to ensure are compliant in your Remote Access Domain. These controls won't meet every compliance goal but will satisfy many current compliance requirements and make your Remote Access Domain more secure.

Best Practices for Remote Access Domain Compliance

The Remote Access Domain opens applications and resources to remote users. Doing so potentially exposes your internal environment to more threats. Because this domain commonly connects remote users to your environment using an untrusted WAN, you must ensure the controls protect your internal resources. Selecting, deploying, and managing the right security controls can provide efficient and secure access across an untrusted WAN.

TABLE 13-2 Common compliance controls in the Remote Access Domain.

TYPE OF CONTROL	COMPONENT	DESCRIPTION
Preventive	Proxy server	Prevent any unencrypted traffic from traveling between remote users and your internal network.
	Firewalls	Use a firewall between the VPN endpoint and your internal network to identify and deny unnecessary traffic.
	User-based access controls for all resources	Restrict access to the VPN to reduce traffic and resource exposure.
Detective	Configuration change control	Limit changes to all network device configuration settings and filtering rules. Require approval for all changes before deploying them.
	Performance monitoring	Frequently sample VPN traffic flow metrics and alert for any unusual activity.
	Traffic analysis	Examine traffic for known attack signatures and to ensure data is encrypted.
Corrective	Configuration settings monitoring	Compare VPN/remote access device configuration settings to stored baselines to detect any unauthorized changes.
	Penetration testing	Conduct periodic penetration tests to identify security control weaknesses.
	VPN/remote access component patching	Keep VPN/remote access devices and applications patched to the latest available level.

Attack intervention	Automatically modify filtering rules to deny traffic from sources generating known attack signature packets.
Business continuity planning and disaster recovery planning	Develop and maintain plans to survive and continue operations in the face of small or large disruptions. Establish alternative WAN access plans in the case of primary WAN failure.

This list of best practices covers the most common suggestions and goals that many organizations have found helpful in securing the Remote Access Domain. These pointers will help you get started to develop a plan and select the right security controls to ensure your remote users enjoy a high level of service without sacrificing your data's security:

- Map your proposed remote access architecture, including redundant and backup connections. Use one of the several available network-mapping software products to make the process easier. Update the network map any time you make physical changes to your network.
- Install at least one firewall between your VPN endpoint and your internal network.
- Select a VPN provider that your clients can easily access. If you select a vendor-specific VPN solution, develop a method to distribute and maintain the VPN client software to your users.
- Use global user accounts whenever possible.
- Use strong authentication for all user accounts.
- Create a limited number of administrative accounts with permissions for remote administration.
- Develop a backup and recovery plan for each component in the Remote Access Domain. Don't forget to include configuration settings for network devices in your backup and recovery plans.
- Implement frequent update procedures for all operating systems, applications, and network device software and firmware in the Remote Access Domain.
- Monitor VPN traffic for performance and suspicious content.
- Carefully control any configuration setting changes or physical changes to domain nodes. Update your network map after any changes.
- Require encryption for all communication in the Remote Access Domain.
- Enforce anti-malware minimum standards for all remote computers as well as server computers in the Remote Access Domain. Ensure all anti-malware software and signature databases are kept up to date.

Review the suggested best practices and implement the controls that work best for your environment. Each organization has different needs and will end up with different controls to best ensure functionality and security in the Remote Access Domain.



CHAPTER SUMMARY

This chapter covered how to enable remote users to access your network's internal applications and resources by implementing components in the Remote Access Domain. You learned to address the increased risks associated with allowing remote users to access your network using untrusted WANs. You also learned about controls and

strategies that work well in the Remote Access Domain to keep your environment functional without sacrificing compliance.



KEY CONCEPTS AND TERMS

Baseband
Broadband
Encapsulating protocol
Hypertext Transfer Protocol (HTTP)
Hypertext Transfer Protocol Secure (HTTPS)
Remote Authentication Dial In User Service (RADIUS)
Secure Socket Tunneling Protocol (SSTP)
Server Message Block (SMB)
Simple Network Management Protocol (SNMP)
Terminal Access Controller Access-Control System Plus (TACACS+)
Tokenization
Tunneling
User Datagram Protocol (UDP)



CHAPTER 13 ASSESSMENT

1. The primary concern for remote access is availability.
 - A. True
 - B. False
2. Which entity is responsible for controlling access to network traffic in the WAN?
 - A. WAN optimizer
 - B. Your organization
 - C. WAN service provider
 - D. Network management platform
3. _____ is the primary security control used in the Remote Access Domain.
4. All VPN traffic is encrypted.
 - A. True
 - B. False
5. Given adequate security controls, PDAs are appropriate for use as remote access devices.
 - A. True
 - B. False
6. Which of the following terms means the process to decide what a user can do?
 - A. Identification
 - B. Authentication
 - C. Clearance
 - D. Authorization
7. Which of the following protocols is used for encrypted traffic?
 - A. HTTPS

- B. SNMP
 - C. IP
 - D. L2TP
8. _____ is a technique that creates a virtual encrypted channel that allows applications to use any protocol to communicate with servers and services without having to worry about addressing privacy concerns.
9. Which of the following protocols works well with firewalls?
- A. GRE
 - B. SSTP
 - C. L2TP
 - D. L2F
10. Which of the following transmission techniques requires the entire bandwidth of a channel?
- A. Multiband
 - B. Baseband
 - C. Broadband
 - D. Duplex
11. _____ is a network protocol used to monitor network devices.
12. The use of global user accounts can simplify user maintenance.
- A. True
 - B. False
13. Which protocol is commonly used to protect data sent to Web browsers when not using VPNs?
- A. IPSec
 - B. PPTP
 - C. GRE
 - D. TLS
14. Which of the following controls would best protect sensitive data disclosure to unauthorized users using remote computers?
- A. Encryption
 - B. Strong passwords
 - C. Firewalls
 - D. Configuration management tools
15. Which protocol does SNMP use to transport messages?
- A. TCP
 - B. UDP
 - C. TLS
 - D. GRE

CHAPTER 14

Compliance Within the System/Application Domain

S

EVERAL DOMAINS SUPPORT distributed applications. Application components can run on different networks and work together to perform business functions. Some application components run in your organization's environment and others run outside your environment. The various domains work together to provide the infrastructure to connect users to resources. There's one more piece to the puzzle, however. To complete the picture, you'll need to learn how distributed application components operate, where they fit into a seamless application design, and how to ensure you maintain your data's security as your application components process and manipulate it.

This chapter covers your applications and the systems that run them. The domain responsible for application software components is the System/Application Domain. This domain provides the computers and the applications that run on them. These application components exchange data with users or other application components and perform some function that is of value to users. In this chapter, you'll learn about the System/Application Domain and how to ensure compliance in this domain.

Chapter 14 Topics

This chapter covers the following topics and concepts:

- How compliance law requirements relate to business drivers
- Which devices and components are commonly found in the System/Application Domain
- What system and application traffic and performance monitoring and analysis are
- What system and application configuration and change management are
- Which system and application management tools and systems are commonly used
- What access rights and access controls in the System/Application Domain are
- How to maximize confidentiality, integrity, and availability (C-I-A)
- What system/application server vulnerability management is
- How to ensure adherence to documented IT security policies, standards, procedures, and guidelines
- What best practices for System/Application Domain compliance are

Chapter 14 Goals

When you complete this chapter, you will be able to:

- Identify compliance law requirements and business drivers
- Compare how devices and components found in the System/Application Domain contribute to

compliance

- Describe methods of ensuring compliance in the System/Application Domain
- Summarize best practices for System/Application Domain compliance

Compliance Law Requirements and Business Drivers

Although sharing resources such as printers and disk drives among network users is beneficial and can reduce costs, the real power of network environments is in distributed applications. Centralizing core business functions on networked servers can dramatically increase the security of your data in many ways. You can centrally control how you store your data and how you allow users to access it.

The System/Application Domain provides the environment for the applications you run as clients on your network and the computer systems that house them. This domain provides the engine for today's distributed applications and enables you to provide individual components of applications as opposed to entire applications in one footprint. [Figure 14-1](#) shows the System/Application Domain in the context of the seven domains in the IT infrastructure.

Keeping data secure in the System/Application Domain involves ensuring availability and controlling unauthorized access. You've already learned about many of the techniques you'll use in the System/Application Domain. Although other domains focus on keeping data secure as it travels across various networks, the System/Application Domain's main security controls ensure your data's security in storage and in use. As with other domains, you'll likely need to show compliance with one or more requirements that directly address the sensitive data you store and process in the domain. The Health Insurance Portability and Accountability Act (HIPAA) requires controls to protect the privacy of medical data, PCI requires credit card privacy controls, and many states require privacy controls on any personally identifiable data. These are only a few of the requirements you'll need to satisfy when selecting security controls for storing and using data. A solid security policy that includes compliance with all appropriate requirements should not only be secure, but should support efficient and cost-effective operation. Implementing the controls necessary to support your security policy in the System/Application Domain makes your organization more effective by providing useful data that is compliant with relevant requirements.

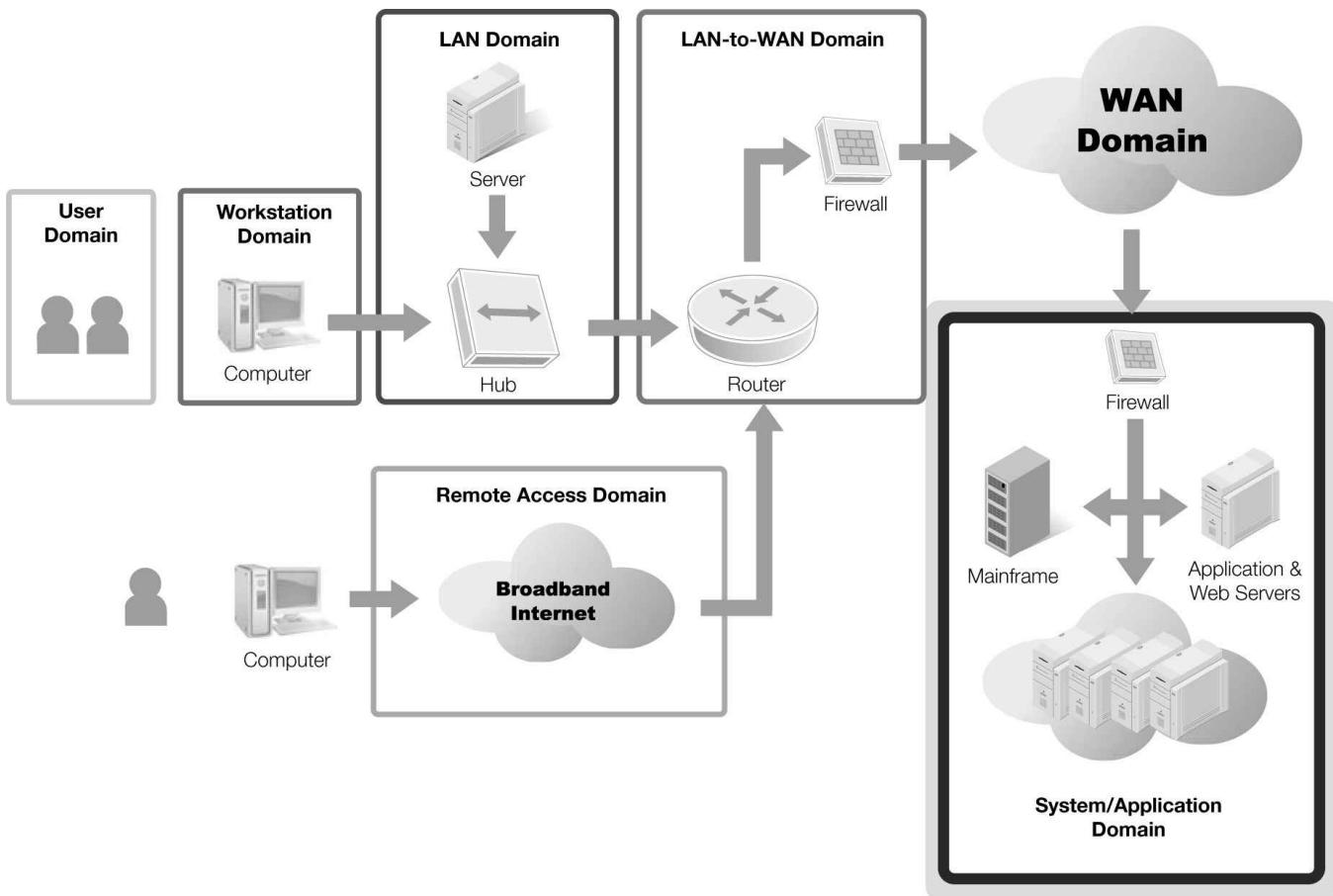


FIGURE 14-1 The System/Application Domain within the seven domains of a typical IT infrastructure.

Protecting Data Privacy

Because the System/Application Domain centralizes much of your data and the processing of that data, it is important that you protect it from disclosure or unauthorized alteration. More and more compliance requirements state that applications must ensure the privacy of different types of data. Recall that ensuring data privacy essentially means allowing only authorized users to view or modify it. Because you control all of the components in the System/Application Domain, you can deploy layers of controls to restrict access to authorized users.

Although controlling access to data and resources can be challenging, in some ways it is a little easier than trying to protect data as you send it to remote locations. You can enforce strict rules that limit which users and programs can access your data. An unauthorized user must access your network, then access a server in the domain, and then run a program or access data in a database. There are several points along the way to place good security controls. You can implement several types of controls that make it difficult for unauthorized users to get to your private data. An important first step is to identify sensitive or private data and then design controls to protect that data.

Implementing Proper Security Controls for the System/Application Domain

The best security controls are simple layered controls. Try to avoid overly complex controls. Complex controls generally require more effort to configure and maintain and often provide more opportunities to fail. Your goal in designing security controls is to ensure they do their jobs and keep your data secure. Although deploying layered controls is generally considered to be sound security practice, be careful that you don't create so many controls that

authorized users have difficulty accessing the data they need. Try to search for controls that balance security and usability.

Security controls in the System/Application Domain generally fall into three categories. There are many potential controls, but the most important controls should isolate data, limit access to data, or protect data from loss through redundancy. Each type of control plays a part in keeping your data secure and your organization compliant:

- **Isolate data**—Because much of an organization's sensitive data resides in one or more databases in the System/Application Domain, it is important to place barriers between sensitive data and other entities. You can use firewalls and your network design to isolate data. Your network addressing scheme can separate one or more nodes into their own subnets. A **subnet** is simply a part of a network. Other network devices, such as switches, can physically isolate subnets from other nodes.

technical TIP

One example of too many controls is the use of multiple logons. As environments grow and add new functionality, it is common to deploy new software applications. Many software applications use their own internal user identification, authentication, and authorization strategies. Using an application with its own defined users poses a few problems. One is that systems administrators face additional maintenance to keep the user list accurate. Another is that users have to log on several times as they use different applications. One solution is to use a single sign-on (SSO) system in which a user only has to sign on, or log on, once. SSO can greatly ease user frustration. It might sound like a minor decision, but it can have a large effect on how well your users accept any new controls.



TIP
Regardless of the operating system or controls you use, limit access to your sensitive data. Know which users and which nodes can access your data.

- **Limit access to data**—Node and user access controls in the System/Application Domain are similar to access controls for other domains. Operating systems provide mechanisms to restrict object access by users or groups. You can also use network authentication to restrict which computers and devices can connect to servers that contain sensitive data.
- **Protect data from loss through redundancy**—Because the System/Application Domain exists to provide applications and data for your users, it has to be functional. You'll need plans to ensure users can access your applications and data regardless of what happens. That means you'll need to create redundant copies of data or employ other strategies to protect your organization from loss of data or functionality.

Several other domains support users and their ability to access applications and data. In one view, you can look at the System/Application Domain as the central repository of the data you are trying to protect. The System/Application Domain provides the security controls closest to your data. An attacker who has compromised enough controls to reach this domain doesn't have much farther to go. The controls you place in the System/Application Domain could be the controls that make the difference between secure data and data loss. Take the time to plan your security controls well.

Devices and Components Commonly Found in the System/Application Domain

The System/Application Domain contains the application components that your organization runs and the computer systems on which the applications reside. This domain also contains computers, devices, and software components that support the domain's application software. The rest of this section lists the devices and components you'll commonly find in the System/Application Domain and some of the controls to ensure compliance. [Figure 14-2](#) shows the devices and components commonly found in the System/Application Domain.

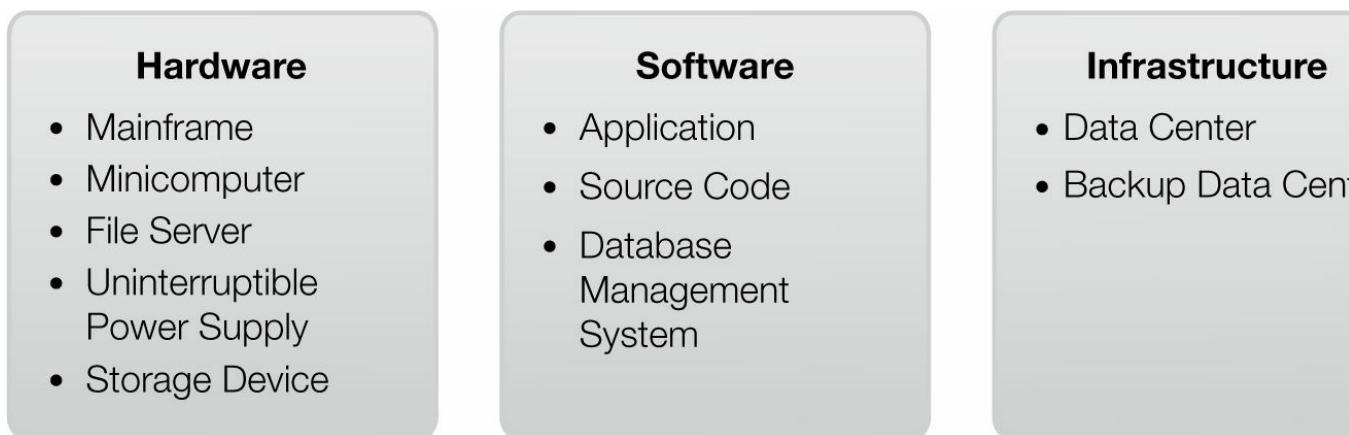


FIGURE 14-2 Devices and components commonly found in the System/Application Domain.

Computer Room/Data Center

The components in the System/Application Domain commonly reside in the same room. The room in which central server computers and hardware reside is called a **data center**, or just a computer room. Because the software and data in this domain are central to your organization's operation, it is imperative that the hardware stays operational. A well-equipped data center generally has at least the following characteristics:

- **Physical access control**—Secure data centers have doors with locks that only a limited number of people can open. Electronic locks or combination locks are common to easily enable a group of people access to the room. Physical access control reduces the likelihood an attacker could physically damage data center hardware or launch an attack using removable media. Inserting a universal serial bus (USB) drive that is infected with malware is one type of attack. Limiting physical access to critical hardware can mitigate that type of attack.
- **Controlled environment**—Heating, ventilating, and air conditioning (HVAC) services control the temperature and humidity of a secure data center. Data centers routinely have dozens or even hundreds of computers and devices, all running at the same time. Keeping the temperature and humidity at proper levels allows the hardware to operate without overheating. Data centers also need dependable electrical power. A data center requires enough reliable power to run all computers and devices currently located in the data center, leaving room for growth.
- **Fire-suppression equipment**—A data center fire has the potential to wipe out large amounts of data and hardware. Extinguishing a fire helps protect the hardware assets and the data they contain. Unfortunately, water could damage computing hardware as

much as fire, so sprinklers aren't appropriate in data centers. A common solution is the deployment of a roomwide fire-suppression gas to displace the oxygen in the entire room.

- **Easy access to hardware and wiring**—Data center components tend to change frequently. Data center personnel must upgrade old hardware, add new hardware, reconfigure existing hardware, and fix broken hardware. Each of these tasks generally involves moving hardware components from one place to another and attaching necessary wires and cables. Data center computers generally don't have cases like desktop computers do. Often they look like bare components on rails. This design allows them to be used in rack systems. A **rack system** is an open cabinet with tracks into which multiple computers can be mounted. You can slide computers in and out like drawers. Using rack systems makes it easy to manage hardware. Because there tends to be a lot of wiring in a data center, many use a raised floor design. Using raised floors with removable access panels makes it easy to access wires and increases the overall airflow throughout the data center.

technical TIP

When designing a disaster recovery plan, always protect people first. Computers, devices, and data can all be replaced. People cannot. A common gas used for years in data center fire-suppression systems is **halon**. Although halon works well to suppress fire, it is hazardous to humans and the environment. Due to the dangers associated with halon, other gas fire-suppression options have emerged to replace it. In fact, the manufacture of a common type of halon, Halon 1301, is banned and all new fire-suppression systems must use an alternative substance.

- **High-speed internal LAN**—Many computers in the data center are high-performance server computers. To optimize communication between servers, high-bandwidth networks, such as fiber optic networks, are common within the data center.

When designing a data center, make sure it can support all the components you need today and in the foreseeable future. Data centers that are flexible and scalable allow your organization to change and grow to reflect business demands.

Redundant Computer Room/Data Center

A disaster recovery plan contains the steps to restore your IT infrastructure to a point where your organization can continue operations. If a disaster occurs that causes damage and interrupts your business functions, it is important to return to productive activities as soon as possible. If your organization can't carry out its main business functions, it cannot fulfill its purpose. A solid disaster recovery plan (DRP) carefully identifies each component of your IT infrastructure that is critical to your primary business functions. Then, the plan states the steps you can take to replace damaged or destroyed components.

Several options are available for serious disasters that damage or destroy major IT infrastructure components. These are a few of the most common options, starting with the most expensive option with the shortest cutover time:

- **Hot site**—This is a complete copy of your environment at a remote site. Hot sites are kept as current as possible with replicated data so switching from your original environment to the alternate environment can occur with a minimum of downtime.

- **Warm site**—This is a complete copy of your environment at a remote site. Warm sites are updated with current data only periodically, normally daily or even weekly. When a disaster occurs, there will be a short delay while a switchover team prepares the warm site with the latest data updates.
- **Cold site**—This is a site that may have hardware in place, but it will not likely be set up or configured. Cold sites take more time to bring into operation because of the extensive amount of configuration work required for hardware and software.
- **Service level agreement (SLA)**—This is a contract with a vendor that guarantees replacement hardware or software within a specific amount of time.
- **Cooperative agreement**—A cooperative agreement is between two or more organizations to help each other in case a disaster hits one of the parties. The organization that is not affected by the disaster agrees to allow the other organization to use part of its own IT infrastructure capacity to conduct minimal business operations. There is usually a specified time limit that allows the organization that suffered damage time to rebuild its IT infrastructure.

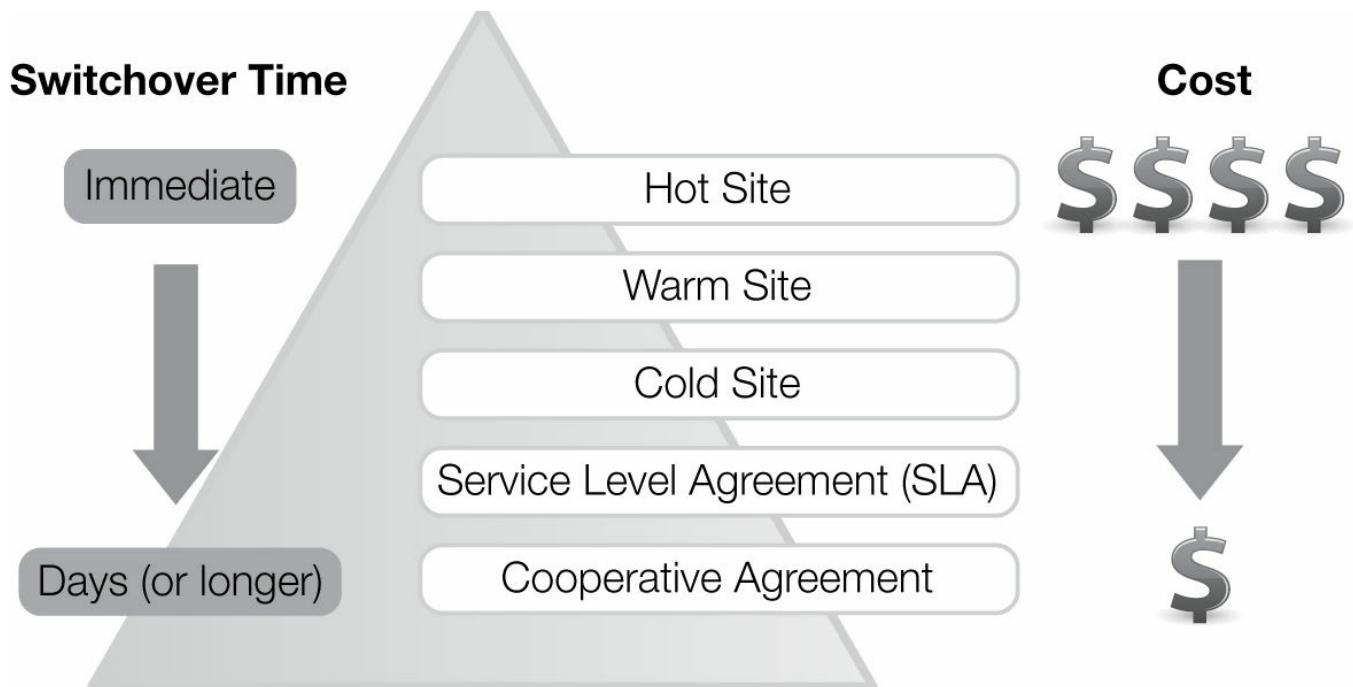


FIGURE 14-3 Disaster recovery options.

Figure 14-3 shows disaster recovery options in terms of switchover time and cost.

Regardless of which option best suits your organization, the purpose of a disaster recovery plan is to repair or replace damaged IT infrastructure components as quickly as possible to allow the business to continue operation.

Uninterruptible Power Supplies and Diesel Generators to Maintain Operations

There is a lot of confusion between a DRP and a business continuity plan (BCP). The two plans work closely with each other and depend on each other for success. You can summarize the difference between the two plans as follows:

- A DRP for IT ensures the IT infrastructure is operational and ready to support primary business functions. A DRP for IT focuses mainly on the IT department.
- A BCP is an organizational plan. It doesn't focus only on IT. The BCP ensures the

organization can survive any disruption and continue operating. If the disruption is major, the BCP will rely on the DRP to provide an IT infrastructure the organization can use.

- A DRP is a component of a comprehensive BCP.

To summarize, a comprehensive BCP will take effect any time there is a disruption of business functions. An example is a water main break that interrupts water flow to your main office. A DRP takes effect when an event causes a major disruption. A major disruption is one where you must intervene and take some action to restore a functional IT infrastructure. A fire that damages your data center is an example of a disaster.

One type of interruption addressed by a BCP is a power outage. If a data center loses power, computers cannot operate and the environment can no longer support the hardware. With no power, there is no HVAC, lights, or anything else that relies on electricity. It is important to plan for power outages and place corrective controls to address a loss of power. There are two main methods that address a power outage. The first method addresses short-term outages, whereas the second method addresses longer-term outages:

- **Uninterruptible power supply (UPS)**—A UPS provides continuous usable power to one or more devices. UPS units for data centers are typically much larger than workstation UPS units and can support several devices for longer periods of time. A UPS protects data center devices from power fluctuations and outages from several minutes to even several hours for large, expensive units.
- **Power generator**—Generators, which commonly use diesel fuel to create electricity, can deliver power to critical data center components for long periods of time. When a power outage lasts longer than a UPS can power devices, generators can produce electricity as long as they have fuel. Generators are generally not extremely long-term solutions. They will provide power until either regular power is restored or you can move to an alternative data center that has reliable power. If you must locate a data center in a place that does not have reliable power, however, generators can become the primary power source.

Mission-critical data centers require multiple levels of protection to ensure continuous operation. UPS devices and generators are integral parts of a BCP that keep an organization in operation.

Mainframe Computers

Several types of computers make their homes in data centers. The largest type of computer is the mainframe computer. The term *mainframe* dates back to the early days of computers and originally referred to the large cabinets that housed the processing units and memory modules of early computers. The term came to be used to describe large and extremely powerful computers that can run many applications supporting thousands of users simultaneously. Mainframe computers also have the characteristic of being extremely reliable. Most mainframe computers run without interruption, and can even be serviced and upgraded while still operating.

Because the hardware, software, environmental requirements, and maintenance for mainframe computers are all expensive, only the largest organizations typically can justify their use. Mainframe environmental and power requirements created the need for early dedicated data centers. Today's mainframe computers are powerful hosts for multiple operating systems that run as **virtual machines**. A virtual machine is a software program that

looks and runs like a physical computer. A large mainframe computer can run many virtual machines and provide the services of many physical computers.

Minicomputers

Many organizations realize they need more computing power than basic workstations or PC-based hardware but aren't ready to commit to a mainframe computer. The first minicomputers started appearing in data centers in the 1960s as an alternative to mainframe computers. Minicomputers are more powerful than workstations but less powerful than mainframe computers. They fit somewhere in the middle and address the needs of medium-sized businesses.

Before the 1980s, minicomputers and mainframe computers were the only types of computers that could handle multiple users and multiple applications at the same time. Smaller computers could only handle single users and one application at a time. The 1980s saw the growth of more capable hardware and operating systems for low-cost computers. These small, inexpensive computers are called *microcomputers* and still dominate the personal computer and workstation markets.

Minicomputers still exist to address the needs of medium-sized businesses but they aren't as common as they were in the past. Some of today's minicomputers are distinct hardware platforms and some are actually high-end microcomputers running operating system versions that cater to high performance and reliability. Either way, minicomputer performance and cost fill a need between workstations and mainframe computers.

Server Computers

Some computers in a data center aren't multipurpose computers but fill specific roles. Computer roles most commonly focus on satisfying client needs for specific services. Computers that perform specific functions for clients are generally called *server computers*, or just *servers*. Common servers you'll find in today's environments may include the following:

- File servers
- Web servers
- Authentication servers
- Database servers
- Application servers
- Mail servers
- Media servers

These are only a few of the types of servers in many data centers. Server computers help organizations by allowing a computer to focus all of its resources on a single task, providing a specific service to clients. A collection of separate server computers, each providing a different service, can increase the performance of the entire environment by removing interservice conflicts and competition for a single computer's resources. Isolating services on separate server computers can also limit the effects of attacks. An attack that compromises a server computer running a single service will have less impact than a compromise of a single computer running many applications and services.

Data Storage Devices

Data centers are convenient places to locate shared storage devices. The central location,

managed environment, and higher general level of security make the data center an ideal environment for protected shared storage. Many networks offer managed storage devices that are shared among network users. Shared devices can be attached to file servers or be separate from server computers. Shared storage devices can be disk drives, tape libraries, optical jukeboxes, solid state storage, or any other mechanism used to store data.

One common method to provide shared storage capability to network users is through the use of a **storage area network (SAN)**. A SAN is a collection of storage devices that is attached to a network in such a way that the devices appear to be local storage devices. In effect, the storage devices form their own network that the operating system accesses just like local drives. The SAN devices protect the data by limiting how clients can access the storage devices. SANs can make it easy to keep shared data available and secure.

Applications

Computer applications have matured along with computer hardware capability. Early computing systems placed all data and software capabilities on a central host computer. Clients used simple terminals to connect directly to the host computer to run applications. Application design has changed through several generations to its current level of maturity, the distributed application model. Each architectural change depended on advances in networking support and changed the way applications use networks and resources. Application architectures mainly differ in the location of critical resources. Critical application resources are as follows:

- **Data storage**—The interface to physical storage devices, such as disk drives
- **Data access**—Software to access stored data, such as database management systems or document management systems
- **Business logic**—Application software that accesses and processes data
- **User interface**—Application software that interacts with end users

Table 14-1 lists major application architectures and their impact on network resources.

Although not all applications are fully distributed, the trend for new development efforts is to deploy distributed applications. More and more applications are specifically written to run on application server computers. This move toward distributed applications has an impact on security and compliance. Although many organizations use application servers in a secure data center to run application components, others may just run applications on a generic network computer. Each application must ensure it protects the security of the data it handles.

TABLE 14-1 Application architectures.

ARCHITECTURE	SERVICE LOCATION				COMMENTS
	Data Storage	Data Access	Business Logic	User Interface	
Host based	Host	Host	Host	Host	Everything runs on the host. Host-based applications are easy to maintain and secure but are not very scalable.
Client based	Server	Client	Client	Client	This architecture is also called diskless workstations. This architecture didn't last too long because even a few clients can saturate a network with all disk accesses occurring over a network.
Client/server	Server	Server	Client	Client	This common model attempts to separate application execution from data access and storage. In a classic client/server model, the client runs all of the application code. Although workstations have become powerful, this model is slow when the application needs large amounts of data that must be transferred across the network.
Distributed	Server	Server	Server	Client	Distributed computing attempts to solve the network saturation problem by reducing the amount of information transferred across the network. Large volumes of data can be transferred between a database server and an application server in the data center without having to use the rest of the network. Reduced network usage can result in much better performance. Keeping more data within the data center's network increases the data's security as well.

technical TIP

Not all source code files are compiled into programs computers can run. Some languages actually interpret source code files, while other environments just assemble source code instructions into machine-readable instructions. Regardless of your particular environment, all programs start off as source code files.

Source Code

Application software is a collection of computer programs that fulfills some purpose.

Programs that computers can run are the result of a process that starts with programmers creating text files for programs, called **source code**. Source code files are then compiled into programs that computers can run.

The process of changing how an application program runs starts with changing the source code files that correspond to the program you want to change. The programmer would then follow the prescribed procedure to convert the source code into a program the computer can run. This process works for attackers as well. Although it is possible to modify a computer program directly, it is far more difficult than modifying the source code. An important step in securing applications is to remove the source code. Without source code, it is very difficult to modify an application.

TIP

The best way to secure applications from unintended changes is to keep your development environment separate from your production, or live, environment. You'll learn more about how to do this in the section that covers configuration and change management. Separating the different environments is mandatory for SOX compliance.

Databases and Privacy Data

Very few applications run as standalone programs. Nearly every application accesses data of some sort. Enterprise applications may access databases that are hundreds of gigabytes or even terabytes in size. Databases that store this much data are valuable targets for attackers and should be the focus of your security efforts in the System/Application Domain. Data is a crucial asset in many of today's organizations. An organization's ability to keep its data secure is critical to its public image and is mandatory to maintain compliance with many requirements.

Because the database is where many organizations store sensitive data, it is the last barrier an attacker must compromise. In a secure environment, an attacker must compromise several layers of security controls to get to the actual database. Even though the hope is that an attacker never gets that far, you should implement additional controls to ensure you protect the data in your database from local attacks. The database should be the center of your security control efforts. You should take every opportunity to restrict access to the sensitive data in your database, including using controls provided by your database management system.

You'll learn about specific database controls in the "Access Rights and Access Controls in the System/Application Domain" section later in this chapter. Just because your database resides in a secure data center, you shouldn't assume it is safe. Use the security controls available to you at every level possible. Your job is to make an attacker's job as difficult as possible.

System and Application Traffic and Performance Monitoring and Analysis

The main goals for implementing distributed applications are to make the components that access and manipulate your data secure, easy, and fast. Making components secure depends on a secure infrastructure and deploying the best security controls. Components that are easy to run depend on a solid interface design. The third goal, to make application

components fast, depends on both good design and proper configuration of the underlying infrastructure.

When you deploy application components, good performance depends on identifying configuration problems and usage issues and addressing them. The most efficient way to identify problems is by monitoring application traffic and performance and comparing sampled metrics with expected performance. There are two main methods you can use to monitor application traffic and performance. The first method uses monitoring tools to sample application network traffic and analyze the packets to ensure your applications are exchanging data efficiently with clients. **Application performance monitoring software** can measure end-user response time for server requests as well as end-user traffic volume. You can set thresholds in the monitoring software's configuration to alert you if your application or your network slows down. Application monitoring software installed on the most important application servers can ensure your applications are servicing end-user requests efficiently and making your data available in a timely fashion. Table 14-2 lists several application monitoring software solutions that work with many different types of applications.

The second method to monitor and manage application performance requires specific knowledge of your application and of the tools available to manage it. Most applications, development languages, and database management systems have tools available to monitor how well the application platform is performing. Explore your application and the tools available to monitor how well it is operating. Application- or development language-specific tools might take more time to learn but might also provide far more detailed internal information you can use to enhance your application's performance.

Regardless of the method you employ, application performance monitoring software and application-specific tools can only help identify problems. Solving the problems requires that you first understand why the problem exists and then how to address it. Poor performance can originate from several different sources. Finding the source of a slow application component can be time consuming and difficult. In many cases, solving application performance problems requires input from analysts, developers, network administrators, and database administrators. The problem can be in any of several places. Application monitoring software and application-specific tools serve to identify the problems that affect your application's availability. Your organization's application performance issue resolution plan should direct the next steps.

TABLE 14-2 Application performance monitoring software.

PRODUCT	WEB SITE
SolarWinds	http://www.solarwinds.com/server-application-monitor.aspx
NetScout nGenius Performance Manager	http://www.netscout.com/products/enterprise/nSAS/Pages/nGenius_Performance_Manager.aspx
Blue Coat Application Performance Monitoring	https://www.bluecoat.com/products/intelligence-center
Radware Application Performance Monitoring	http://www.radware.com/Products/APMI
ManageEngine Applications Manager	https://www.manageengine.com/products/applications_manager/

System and Application Configuration and Change Management

Any organization that develops or modifies software applications must follow a configuration management method to ensure the integrity of their software. Far too many organizations lack the formal procedures to control changes to their software. Compliance requires formal change procedures. For example, SOX requires that any changes made to software be documented and tracked in such a way that changes can be undone. Further, SOX requires that all development activities and personnel be completely separate from your production environment. Although compliance requires these actions, they are really just good practices.

Software development and maintenance have evolved as more of an art than a science in many organizations. Small organizations with very few software developers commonly approach the development process informally because it is easy to keep track of a few programs and a few people. As an organization grows, the software development and maintenance activities become more complex. It becomes evident that informal procedures no longer provide the level of control needed to maintain a dynamic application's integrity. One formal method to control the software development life cycle is **software configuration management (SCM)**. SCM provides the activities and requirements to formalize the entire software development process.

SCM requires that all development occur in a separate environment from production. In the most secure environments, the development area is on a server separate from where the completed application runs in production. When developers complete software changes, the changes should move to an isolated testing and quality assurance (QA) environment. Testing and QA personnel test modified software to ensure it complies with the change request requirements and with existing application requirements. Many software changes to fix bugs or add functionality actually cause unintended problems. It is the responsibility of the testing and QA personnel to validate that the newly modified software performs as intended.

Once software changes have been tested and approved, they can be moved into production. Sarbanes-Oxley requires complete separation between developers and the production environment. Software developers are not allowed to access the production environment at all. Another role, such as a configuration gatekeeper, must move the software to the production environment. This security control limits the ability for software developers to accidentally place untested software in production. Untested code could violate any or all of the three C-I-A properties of data security. The separation between developers and production also stops malicious software developers from placing unauthorized software in production environments.

Regardless of your operating or development environment, it is imperative that your organization implement software configuration management software and controls to manage any changes to software. A solid set of tools will help manage changes, keep untested software from harming your data, and make it far easier to remove and replace offending software if an undiscovered bug does end up in the production environment.

System and Application Management, Tools, and Systems

Managing the components of the System/Application Domain means ensuring that the computers and devices are operating properly and that the application components are

running efficiently. These tasks can be grouped into the following goals:

- Ensure your computers and devices are operating properly.
- Ensure your data center network is operating properly, including interfaces to the networks outside your data center.
- Ensure your application components are operating properly.

Proactive monitoring provides assurance that everything is working as planned and raises alerts anytime issues are identified. Application performance monitoring software is the highest-level monitoring and analysis tool. If your application performance monitoring software reports that all is well, you have the assurance that application components, networks, and computers and devices are all operating properly. If a component has issues, your applications won't operate properly. Although it is possible that an issue can develop that does not immediately manifest an application problem, most application performance monitors can periodically run basic tests on idle applications to ensure that all is well.

If your application performance monitoring software does indicate a problem, the course of action may include any of the following:

- Alert appropriate personnel to initiate troubleshooting procedures on the problematic application.
- Launch network monitoring and analysis software to evaluate network components and connections.
- Launch system monitors or interrogators to evaluate data center computers.

The tools you can use include application performance monitoring software as well as system and network monitoring software. Managing computers, devices, networks, and software in the System/Application Domain doesn't introduce any new tools or topics. The practice of ensuring domain components are operating properly consists of tools and techniques that are appropriate and in use for other domains as well. Using these tools and techniques can help ensure the System/Application Domain is providing your users with application components to fulfill business requirements.

Access Rights and Access Controls in the System/Application Domain

The System/Application Domain is perhaps the most protected domain in relation to users. Both local and remote users must pass through several domains to access any components in the System/Application Domain. That means it is reasonable to expect users and attackers to have already encountered several layers of security controls to make it this far. Recall that a good security plan involves several layers of controls. You should deploy solid controls that protect each domain. However, it isn't good enough to rely on security controls in other domains. Although it is reasonable to expect the System/Application Domain components to be relatively safer than Internet-facing components, you still must protect all components in each domain.

What happens if an attacker compromises the security controls in other domains and access the System/Application Domain components? How can you stop an attempted attack? The answer to both questions is to ensure you limit access to each component in the System/Application Domain using security controls. Although this might seem obvious, it is important to secure each domain's components and resist relying on controls in any other domain. Even if you properly secure your environment using multiple layers of controls,

always assume the current domain must protect each component. When each domain provides security controls that protect its components without interfering with business processes, you automatically implement a layered approach to security that makes your environment more secure.

Although the System/Application Domain is farther away from users and tends to be more protected than some other domains, it does have a particular weakness. Distributed applications commonly depend on the Internet to expose application components to the widest number of remote users. By far, the most common method to make application components available to remote users is through a Web server. The Web server allows Internet users to send requests for services. Your application design dictates whether your application is public or private. Private applications tend to be easier to protect because you have the option of requiring a secure VPN to access your application. Most public applications allow non-VPN users to request services.

Allowing anonymous Internet users into your network poses a potential problem. To illustrate, [Figure 14-4](#) shows a remote user requesting and receiving service from a distributed application. The process is as follows:

1. Anonymous users can send an application request directly to your Web server. Your Web server likely resides in the demilitarized zone (DMZ) in your LAN-to-WAN Domain.
2. The Web server launches a program that establishes a connection to an application server in the System/Application Domain.
3. The application server runs the requested program on behalf of the remote user and returns the results through the Web server.
4. The Web server returns the results to the user.

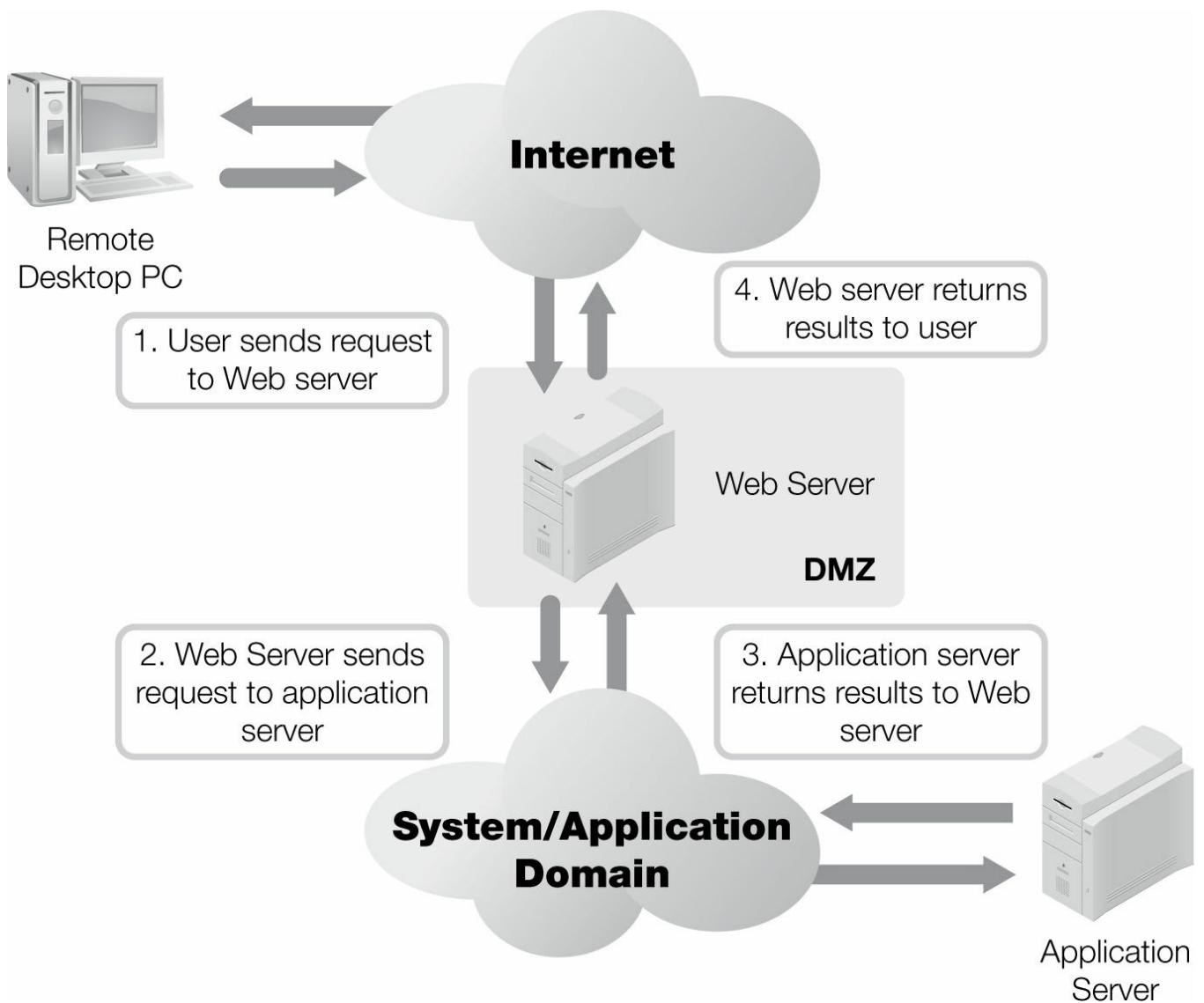


FIGURE 14-4 Remote user request for a service from a distributed application.

Following the path, it is easy to see that an attacker can get right to your Web server in the DMZ. To make your distributed application available to the maximum number of people, your firewalls will likely leave your Web server ports wide open. All an attacker has to do is compromise your Web server to potentially connect right to your application server. One well-placed attack can threaten your System/Application Domain. That's why having layered security controls in every domain is essential.

Your System/Application Domain should implement access controls for nodes and users. You should use Network Access Control (NAC) software, such as PacketFence or Sophos NAC Advanced, with positive authentication to ensure no rogue nodes are allowed to access System/Application Domain components. To address attacks from your Web server, your application server should enforce user access controls. In addition, your application should enforce its own user access controls. You should define one set of users for remote access through a Web server and another set of users for internal access. That way, you can separate the rights and permissions and also audit remote user access more aggressively. The most secure position is to assume all access requests are potentially hostile and then evaluate each one with aggressive access controls.

► NOTE

In many cases, addressing the C-I-A properties of data security meets compliance requirements as well. Don't neglect to review your compliance requirements when examining security controls, as some requirements might call for additional security controls.

Maximizing C-I-A

Identifying security controls to protect data can be confusing. As with other domains, one effective way to ensure you have the right controls in place is to review how well you are maximizing the C-I-A properties of data security. If you can demonstrate that your controls are addressing the needs for data confidentiality, integrity, and availability, you have addressed the basic needs for data security.

BCP and DRP

The first concern for your System/Application Domain is that the data be available to authorized users on demand. That means all the necessary computers, devices, and networking components must be operating properly and any software required for your application should be up and running. When your data is not available, you need to have a plan in place to address the problem. Most security-related legislation, regulations, and standards require some type of business continuity plan (BCP) to ensure data availability.

A BCP takes effect any time some event interrupts your business operation. Events can be minor, such as a brief power outage, or major, such as a fire in the data center. In either case, your BCP should contain the steps to restore business operations back to normal. In some cases, a disaster causes damage to one or more infrastructure components that interrupts your BCP activities. For example, a fire in the data center might destroy a server. Until you replace or repair the server, it cannot contribute to your business operation. You need another plan to address disasters that restores your operating environment to a state where it can contribute to your business operation.

The disaster recovery plan (DRP) is a separate plan that responds to disasters and restores the infrastructure components to a point where the BCP can restore business operation. Both plans are important. You must ensure you provide recovery teams with the material and information they need to execute a DRP and BCP when needed.

The most important two resources any recovery team needs are well-documented procedures and redundant, undamaged domain components. Redundant, undamaged domain components can be any of the following items:

- Current valid backup images of data and other files
- Current replicated images of data and other files
- Identical copies of hardware and devices, either individual components or an entire duplicate data center
- Replacement hardware and devices
- Replacement parts for hardware and devices
- Repaired hardware and devices

As long as the recovery team has access to the domain components it needs to restore operation, team members can follow a well-documented plan. Make sure you protect every domain with a comprehensive BCP and DRP.

Access Controls

Access controls play an important part in the System/Application Domain. Earlier in this chapter, you learned how an attacker could compromise your Web server and attempt to access System/Application Domain components directly. If an attacker is able to compromise a computer in your DMZ and exploit a vulnerability that provides access into another domain, solid access controls can limit the damage that attack can do. Many attackers will attempt to escalate user privileges to establish a connection to another computer or another domain to alter or access data.

technical TIP

Your access controls should carefully limit which users can connect to servers in the System/Application Domain from a Web server. Do not allow users with escalated privileges to connect from your DMZ. Only allow escalated-privilege users to connect from a protected Web server that can be reached only by VPN. These controls reduce the potential for an attacker to connect to sensitive servers from Internet-facing components.

In addition to NAC devices limiting connections to System/Application Domain components and operating system access controls for user logons, all applications should implement access controls. Application access controls can limit access to specific data elements. In a database environment, applications can employ access controls at the record or row level. For even more fine-tuned control, some applications and databases support access control at the field or column level. Application controls can limit which users can read data and which users can write data. Proper use of access controls at all levels can protect the confidentiality and integrity of your data. As long as you employ strong authentication techniques, user identity and access controls help keep your data secure.

Database and Drive Encryption

Access controls protect the confidentiality and integrity of data as long as the operating system enforces the controls. If an attacker is able to acquire a copy of data outside the scope of the operating system, access control cannot protect the data's security. There are two main ways to acquire data outside the scope of the operating system.

The first attack method is to boot the computer that contains the data using removable media. Removable media, such as a CD, DVD, or USB drive, can contain an alternative operating system that allows the attacker to access any file with no access controls. A successful attack such as this allows an attacker to copy any desired data, regardless of how confidential it is. There are two main defenses to this type of attack. The first defense is to limit physical access to critical servers. Most data centers employ physical controls such as locked access doors that only a select few people can open. If an attacker cannot physically access a computer, this type of attack fails. The second defense is to employ operating system-level encryption.

A second type of attack can result in accessing large amounts of confidential data. This second type of attack involves acquiring a copy of a backup image. Many organizations make the mistake of not securing backups once they are created. You should transport backup media to another physical location to protect it from a physical disaster. The purpose of creating backup images is to provide a redundant copy of your data if a disaster destroys the primary copy. Suppose a flood destroys your entire data center. If your backup images

were stored in the data center, they could be destroyed as well. Transporting backups to remote locations for storage increases the likelihood they'll be usable even after a disaster at the main data center. If an attacker can steal a copy of your backup media as it is being transported from the data center to the storage location, all of your data could be revealed. Data on backup media is easy to access.

There are at least two controls to stop this type of attack. The first control is to secure all backup media during transport. Treat backups with care. Investing in a method of secure transportation is far less expensive than one security breach. Many companies provide secure transportation and storage for backup media. Consider using such a service to ensure your backups don't fall into the wrong hands. The second control to protect backups is to use data-protection methods such as encryption or tokenization. There are several types of encryption and tokenization solutions available for different needs. Some protect entire backup media or files on a disk while others protect individual data elements. [Table 14-3](#) compares the six most common options for data protection.

Protecting data by such means can help ensure only authorized users can access the data. This type of control assists you in protecting the confidentiality and integrity of your data.

TABLE 14-3 Common options to protect data.

PROTECTION TYPE	DESCRIPTION	WHAT IT PROTECTS
File encryption	Encrypts individual files. If the file encryption is part of the operating system, such as Windows Encrypting File System (EFS), the encryption key is derived from the user password and files are not readable when the user is not logged on.	Alternate boot attacks or any attack that bypasses operating system access controls
Folder/directory encryption	Encrypts entire folders/directories. An example is Windows EFS in folder encryption mode.	Alternate boot attacks or any attack that bypasses system access controls
Volume/drive encryption	Encrypts entire volume or drive, such as Windows BitLocker or TruCrypt.	Alternate boot attacks or any attack that bypasses system access controls
Application encryption	Encrypts individual pieces of data based on the application's requirements.	Any attack that bypasses the application access controls; also protects backups from attack
Database encryption	Encrypts the entire database. If implemented by the database management system, this is often called Transparent Data Encryption (TDE).	Any attack that bypasses the database management system access controls; also protects backups from attack
Backup encryption	Encrypts backup media as you create the backup image.	Protects backups from attack
Tokenization	A different approach from encryption. Replaces sensitive values with fake data that looks and behaves like the real data element. This helps to maintain business processes and the usability of the data.	Protects individual data elements from a wide range of threats.

System/Application Server Vulnerability Management

No software is perfect. All software, whether an application or an operating system, is susceptible to software vulnerabilities. Because today's applications and operating systems

are so complex, it is likely that multiple vulnerabilities exist in any version. Attackers know how difficult it is to develop secure software and they expend substantial effort trying to find vulnerabilities to exploit.

Software developers are engaged in a continuous cycle to keep their software as secure as possible. Attackers run exhaustive tests against software to uncover any vulnerabilities. When they find a vulnerability, they develop an attack that exploits it. They launch an attack and some computer systems become victims. The victims report what has happened to the software provider and the software provider modifies its software to remove the vulnerability. The software provider tests its new software and releases it as a patch. Then the cycle repeats itself. Attackers are continuously looking for vulnerabilities and software providers are continuously fixing the vulnerabilities they find.

Operating System Patch Management

Operating systems have substantial access to the hardware they control. Compromising an operating system basically means owning that computer. An attacker who successfully compromises an operating system can often use that computer for other attacks as well. You should frequently check your operating system's Web site for newly released patches and apply those patches. An operating system that has the latest available patches is less vulnerable to the newest attacks.

Set up each computer to download and apply patches automatically or set up a procedure that ensures you apply operating system patches to all computers as soon as they are available. The longer you delay patching any computer, the longer that computer remains vulnerable to newly released attacks.

Application Software Patch Management

Application software can contain vulnerabilities as well. As with operating systems, it is advisable that you acquire the latest application software patches from your application software vendor and apply them as soon as possible. This process is relatively easy for off-the-shelf software. It can be more difficult for software you have modified. Regardless of the role you play in modifying application software, it is important to have a plan in place to keep your software free from known vulnerabilities. Remember, if you know about a vulnerability, chances are some attacker knows about it too.

Adherence to Documented IT Security Policies, Standards, Procedures, and Guidelines

Adherence to documented policies, standards, procedures, and guidelines is important to achieve compliance and a secure environment. That goal is just as important in the System/Application Domain. Although most of the other domains in the IT infrastructure are similar to domains in other organizations, the components in the System/Application Domain tend to be very specific to each organization. The applications any organization runs define the services that organization can provide. In some ways, the System/Application Domain defines the organization to the outside world.

Because the components in this domain are so specific to the organization, in many cases it is imperative to create specific documents to direct actions that apply to the System/Application Domain. Security policies state high-level goals for security. Standards state specific performance metrics to meet goals. Procedures document the steps to meet

stated performance metrics. Guidelines provide general direction for situations that don't have specific procedures. Develop documents that address each of the three C-I-A data security properties and each compliance requirement. Plan how you're going to meet compliance requirements before taking action.

After you take the time to create the documents to direct IT activities, you should make every effort to follow the documents. If they have errors or need to be updated, make the necessary changes to keep them as current as possible. Following documented actions will always result in behavior that is more secure and compliant than simply making it up as you go.

Best Practices for System/Application Domain Compliance

The System/Application Domain is the engine for your organization's distributed applications. Although other domains are crucial to supporting your organization, the System/Application Domain houses most of your organization's data and the programs that access it. Think of this domain as the last chance you have to protect your organization's data from attackers. Although a good layered security plan should prevent attackers from ever getting this far, never assume this domain is safe. Treat it like all other domains and select security controls as if this was the only domain.

Although no single list can include all controls your organization will implement for the System/Application Domain, there are some best practices that organizations have developed through experience. These provide a good starting point for you to plan for a secure and compliant domain. Here are general best practices for securing your System/Application Domain:

- Establish physical controls to protect the data center. Use door locks to limit access to authorized individuals. Install a fire suppression system. Ensure electrical and HVAC facilities meet or exceed your equipment's requirements.
- Use at least one firewall to limit network traffic from other domains to only authorized traffic.
- Use NAC devices to restrict which computers and devices can connect to System/Application Domain components.
- Connect critical server computers using high-speed network media, such as fiber optic, for servers that require large network transfers. An example is the connection between an application server and a database server.
- Define user- or group-based access controls for each computer in the domain.
- Use application-defined access controls to limit access to data.
- Allow low-privilege users to establish connections only between Internet-facing servers in the DMZ and System/Application Domain servers.
- Allow only escalated-privilege user connections that originate from protected Web servers, where users can connect only using a secure VPN.
- Frequently update operating systems with the latest security patches on all computers.
- Frequently update all application software with the latest security patches.
- If your organization engages in software development or software modifications, follow these best practices:
 - Use configuration management software to control software changes.
 - Create separate environments for development, testing, and production.

- Prohibit developers from accessing the production environment.
- Follow formal procedures for approving software to move from development to testing, and from testing to production.
- Create a BCP and DRP that include each component in the System/Application Domain. Keep the BCP and DRP up to date to reflect any changes to the domain. Test the BCP and DRP at least annually.
- Protect all backup media in transit and storage.
- Ensure all backup media is encrypted.
- Encrypt all sensitive data when it is stored on disks.
- Use application monitoring software to identify performance or availability issues.



CHAPTER SUMMARY

A secure distributed application is the result of careful planning and the right security controls deployed in all domains. Because the System/Application Domain is where much of your data and applications reside, it is a good starting point for security controls. If you carefully ensure each component is protected from attacks, you can greatly increase the ability of your organization to support the three C-I-A properties of data security. Ensuring your data is secure in the System/Application Domain is the first step in ensuring its security throughout its life. Follow the best practices, and you'll be on your way to creating and maintaining secure data and processes that meet your compliance requirements.



KEY CONCEPTS AND TERMS

Application performance monitoring software
Data center
Halon
Rack system
Software configuration management (SCM)
Source code
Storage area network (SAN)
Subnet
Transparent Data Encryption (TDE)
Virtual machines



CHAPTER 14 ASSESSMENT

1. The main concern of data security in the System/Application Domain is integrity.
 - A. True
 - B. False

- 2.** Because the System/Application Domain is the innermost domain, security controls are not as important.
A. True
B. False
- 3.** A solid multilayered security plan means that an attacker will likely encounter several security controls before reaching the System/Application Domain components.
A. True
B. False
- 4.** A(n) _____ is a subdivision or part of a network.
- 5.** Which of the following is *not* a common feature of a data center?
A. Controlled environment
B. Limited physical access
C. In-room generator
D. Raised floor
- 6.** Every disaster recovery plan should protect _____ first.
- 7.** Which type of plan contains instructions on how to recover from a power failure?
A. DRP
B. BCP
C. SLA
D. TDE
- 8.** Which of the following is true?
A. A BCP is normally part of a DRP.
B. A BCP addresses only IT issues.
C. A DRP is normally part of a BCP.
D. A DRP should address even minor interruptions.
- 9.** Which common term originally referred to the large cabinets that housed the processing units and memory modules of early computers?
A. Core rack
B. Rack system
C. Mainframe
D. Minicomputer
- 10.** A(n) _____ generally resides in the DMZ and provides the interface between remote users and an application server.
- 11.** Which type of full database encryption doesn't require any user interaction?
A. TDE
B. OLE
C. AES
D. DES
- 12.** Which benefits do application performance monitoring software provide? (Select two.)
A. Measure end-user response time.
B. Measure senior management browsing habits.
C. Measure end-user traffic volume.
D. Measure application-installed code base.
- 13.** According to SOX requirements, which type of user accounts are prohibited from accessing the production environment?
A. Database administrators
B. Software developers
C. Network administrators

D. End users

Beyond Audits

CHAPTER 15

Ethics, Education, and Certification for IT Auditors

CHAPTER 15

Ethics, Education, and Certification for IT Auditors

A

CAREER IN INFORMATION TECHNOLOGY (IT) AUDITING is both rewarding and

demanding. The field continuously evolves and changes. Corporate events of the past, such as the WorldCom and Enron scandals, have forced auditors to adapt to new laws and regulations. Organizations depend on people and data. Employees process, store, and transmit data every day. Organizations must protect the data they use and create, either by law or as a best practice. Therefore, IT information security touches nearly all parts of an organization, and auditing is an important part of security.

A combination of IT and business acumen will continue to drive the auditing profession. Many IT professionals routinely work with IT auditors. At the same time, IT auditors continue to become more technically savvy. Even traditional auditors are increasingly working together with IT auditors and IT professionals.

Having IT auditors with strong values and ethics is more important than ever. IT auditors require in-depth knowledge and skills in the areas of auditing and IT. In addition, IT auditors require traditional soft skills. The IT auditing profession draws on a wealth of resources beyond formal college coursework. A number of professional bodies provide standards and guidance as well as educational and certification programs. The Certified Information Systems Auditor (CISA) and Certified Information Systems Security Professional (CISSP) certifications are two commonly held credentials by IT auditors.

In this chapter, you will learn about certifications and careers in the auditing profession. You will also examine professional ethics and codes of conduct that auditors are required to uphold.

Chapter 15 Topics

This chapter covers the following topics and concepts:

- What IT auditing career opportunities are available
- Why professional ethics and integrity are important for IT auditors
- What codes of conduct exist for employees and IT auditors
- How to become certified or accredited for IT auditing

Chapter 15 Goals

When you complete this chapter, you will be able to:

- Identify the required skills and knowledge for a career in IT auditing
- Understand what makes up a code of conduct and a code of ethics

- Identify codes of ethics from various professional organizations
- Identify the components that make up a mature code of conduct and why organizations establish them
- Understand the differences between auditing associations and other professional bodies
- Differentiate between certifications available to auditors and IT professionals
- Identify educational opportunities and resources available to IT auditors

IT Auditing Career Opportunities

The growth of IT auditing over the last several years is a result of several factors. Two primary factors are new legislative requirements and the use of IT throughout business. Many organizations must prove they have reasonable controls in place, as mandated by legislation such as the Sarbanes-Oxley (SOX) Act and the Health Insurance Portability and Accountability Act (HIPAA). In addition, organizations increasingly rely on computer systems to create, process, and store sensitive data. As a result, new risks and greater challenges have emerged.

Traditionally, organizations relied on **certified public accountants (CPAs)** or auditors associated with accounting to review their financial controls. With the increased use of computing systems, IT departments also began reviewing the adequacy of internal controls. Today, the accounting and information security (IS) fields are common paths to IT auditing careers. Other common paths come via risk management and project management.

Many universities now offer specialized programs in information systems and auditing. Degree-granting programs in information systems security are more common than in the past, as are business accounting programs with a focus on technology. ISACA provides Model Curricula for IS Audit and Control to foster information system auditing degrees in universities. It provides a framework for schools to map courses to topics that provide graduates with the skills and capabilities they need to enter the profession.



TIP

ISACA is a member-based organization for information governance, control, security, and audit professionals. Membership in ISACA provides networking opportunities with a like-minded community. Full-time students can join ISACA at reduced rates. Those interested in IT auditing or IT careers in governance, risk management, control, and compliance might want to consider a membership in ISACA.

In addition to accredited programs, there are numerous professional certifications and associations. These associations provide continuing education and opportunities. Many of these will be covered later in this chapter, including details about certification programs.

One organization, the **Institute of Internal Auditors (IIA)**, provides a fellowship program for experienced auditors to develop their careers. This program encourages audit executives and leaders to send high-achieving auditors through a six-month rotational fellowship program. Participants use their knowledge and desire to support the IIA to conduct research, develop guidance, and create tools and services for the internal auditing profession.

Participants must meet the following requirements:

- At least five years of professional experience in internal auditing

- An active IIA membership or a professional certification
- A bachelor's or higher degree
- Two professional recommendations
- A personal letter of interest
- A minimum of two writing samples
- A completed application

A successful career in IT auditing requires knowledge and skills in both IT and auditing. Numerous certifications exist that focus on IT auditing. Certification exams provide goals for those entering the field, as well as proof of knowledge for experienced auditors. IT auditors should also have an understanding of business concepts. This includes financial and operational controls. Beyond IT and auditing skills, IT auditors require the following soft skills:

- **Analytical**—For analyzing procedural and technical controls, procedures, and processes
- **Communication**—For discussing and presenting audit scope, findings, and recommendations
- **Interviewing**—For gathering required documentation and evidence to conduct an audit
- **Negotiation**—For discussing with management the need to implement identified recommendations
- **Business writing**—For writing effective reports
- **Behavioral**—For dealing with all levels of personnel within an organization throughout the audit process
- **Project management**—For managing the audit process, which is essentially a project
- **Leadership**—For managing a team of IT auditors

In addition to technical, audit, and soft skills, other attributes are helpful. The profession demands that IT auditors appreciate learning and be intellectually curious. In addition, an IT auditor should be objective and highly ethical.

With changing regulations, business challenges, and technology that evolves at a rapid pace, the demand for IT auditors will likely continue. Organizations' increased attention on IT governance, compliance, and risk-management practices will provide many opportunities for the IT auditor.

For college graduates, a career in IT auditing presents a welcome opportunity. In fact, all of the Big Four audit firms have hiring programs for college graduates. These organizations are among the world's largest recruiters of college graduates. If you find you lean more to the technical side, many consulting and security assessment firms offer auditing positions. These positions tend to focus more on the technical aspects of controls and compliance.

Professional Ethics and Integrity of IT Auditors

Ethics are moral beliefs and rules about what is right and what is wrong. Professional ethics relate to any professional field, not just IT auditing. An individual within a professional role has special knowledge. This knowledge can be abused or used for morally unjust purposes. Ethics help to guide the use of this knowledge.



WARNING

Enron is one example of an organization in which much ethical wrongdoing occurred. When scandals such as Enron are uncovered, the results include prison time, fines, and/or bankruptcy. They also negatively affect the lives of the victims.

A **code of ethics** for IT auditors and organizations is important for outlining clear expectations. It also provides the grounds for complaints and possible follow-up disciplinary action. Expectations provide morally acceptable values and principles to help shape behaviors. A code of ethics isn't always enough, however. Consider Enron. Both Enron and its accounting firm, Arthur Andersen, had detailed codes of ethics. Although having codified ethics is important, organizations need to promote ethical behavior as part of the work culture. Having dedicated ethics officers and conducting regular ethics training is a start.

IT auditors need to practice strong ethical behavior and demonstrate integrity and objectivity. Nearly all organizations that provide IT auditing services have their own codes of conduct and ethical standards. Professional organizations for IT auditors, such as ISACA and the IIA, also have codes of ethics.

The IIA's **International Professional Practices Framework (IPPF)**, for example, includes a code of ethics, among other professional guidance. The IIA code of ethics has four principles:

- **Integrity**—Honesty and standing firm to moral obligations helps to establish trust. This is critical as organizations rely on auditors' professional judgment.
- **Objectivity**—Auditors need to make a fair assessment of activities and processes being examined, without being unjustifiably influenced by their own or others' interests.
- **Confidentiality**—Like therapists who are privy to the personal details of their clients, auditors are entrusted with access to valuable information about their client organizations. This information should not be disclosed without proper authority or other legal obligation.
- **Competency**—Auditors are successful in their duties by applying their knowledge, skills, and experience to their work.

The IIA rules of conduct provide further interpretive guidance of the principles to help guide ethical behavior.

The ISACA Code of Professional Ethics has the same intent as the IIA code of ethics, and shares similar concepts and terminology. ISACA's ethical code helps guide both the professional and personal conduct of its members as well as holders of ISACA credentials. ISACA certifications are discussed later in this chapter. The ISACA Code of Professional Ethics contains seven guiding principles. The ISACA published principles state that members and ISACA certification holders shall:

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

- 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.
- 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.
- 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.
- 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.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measures.¹

ISACA also publishes “Professional Ethics and Standards Document #S3” as part of its Information Technology Assurance Framework (ITAF). The S3 standard provides further rules regarding expected behavior. If, for example, adherence to professional ethics is “impaired or appears impaired,” the auditor should consider withdrawing from the assignment. In addition, auditors and ISACA members should make sure the rest of their team adheres to the Code of Professional Ethics. This standard also references additional information system auditing guidelines from ISACA for further information on professional ethics and standards.

Codes of Conduct for Employees and IT Auditors

The terms **code of conduct** and *code of ethics* are often used interchangeably. There are subtle differences, however.

The Sarbanes-Oxley Act defines a code of ethics as “such standards as are reasonably necessary to promote: 1) honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships; 2) full, fair, accurate, timely and understandable disclosure in the periodic reports required to be filed by the issuer; and 3) compliance with applicable government rules and regulations.”

The International Federation of Accountants (IFAC) provides a working definition of a code of conduct in its *International Good Practice Guidance: Defining and Developing an Effective Code of Conduct for Organizations*. IFAC defines a code of conduct as “Principles, values, standards, or rules of behavior that guide the decisions, procedures, and systems of an organization in a way that: a) contributes to the welfare of its key stakeholders and b) respects the rights of all constituents affected by its operations.”

A code of conduct should be consistent with the code of ethics. The code of conduct is often part of the larger ethics and compliance program within an organization. A well-rounded code of conduct does the following:

- Clearly states the company's mission
- Includes a statement from senior management
- Stresses the company's values and principles

- Provides guidelines on ethical and expected conduct, including rules of conduct
- Provides examples of ethical and unethical behavior

IT auditors belonging to professional organizations or holding certifications are required to adhere to professional codes of ethics. Standards set forth by these organizations further guide the conduct of IT auditors. In addition, most organizations, including all of the major accounting and consulting firms, have employer-driven codes of conduct.

Employer-/Organization-Driven Codes of Conduct

Companies listed on public stock exchanges are, in many cases, required to adopt a code of conduct. Both the NASDAQ and the New York Stock Exchange (NYSE) require this. Specifically, they require that listed companies implement and make available to the public their code of conduct for all directors, officers, and employees.

Requirements aside, a code of conduct provides organizations with several benefits. First, it enhances the organization's values and beliefs, and it helps establish a strong culture based on the vision and mission of the organization. Next, a well-implemented code of conduct will build respect as well as enhance the organization's reputation. Finally, it will help guide the organization and its people away from unethical and illegal behavior.

An organizational code of conduct might be included in the employee handbook. Additionally, policy should establish that employees confirm they have read and will comply with the code of conduct. Organizations should reinforce the code occasionally. Many organizations accomplish this through annual verification as well as ongoing training.

NOTE

All employees, including auditors, are expected to comply with their organization's code of conduct. Auditors, however, are also responsible for verifying and testing their clients' codes of conduct.

For example, KPMG is one of the largest auditing firms in the world. The company's code of conduct states that it "sets forth our core values, shared responsibilities, global commitments and promises. Additionally, the code provides you with general guidance about the firm's expectations, situations that may require particular attention, additional resources and channels of communication, as well as illustrative questions and answers." The guide is a colorful, easy-to-read pamphlet available for download from <http://www.kpmg.com/US/en/about/Documents/kpmg-code-of-conduct.pdf>. The Code of Conduct includes the following key sections:

- **Letter from the Chairman**—This introduces KPMG's goal of being regarded as the best Big Four public accounting firm. It further reiterates the strong corporate commitment to an ethics and compliance program to achieve that goal. The letter also introduces the company's "values-based" culture.
- **Our Code and Our Commitment**—This introduces KPMG's commitment to the code, written by another senior executive. It also summarizes the importance of the code and to whom it applies.
- **Our Core Values**—This describes the "KPMG way," which defines the company's culture by identifying values that reflect who it is, what it does, and how it does it.
- **Shared Responsibilities**—This provides key policies and responsibilities for which

individuals and management are held accountable. This section describes ethics and integrity as the foundation of business conduct.

- **Getting Help**—This sets the expectation that help should be sought if necessary and that unethical and illegal activity must be reported. It also reiterates the conduct, policies, and processes around providing an environment that fosters such expectations.
- **Our People**—This reiterates the importance and value of people and the need to embrace diversity and treat each other with respect.
- **Our Firm**—This outlines expected behaviors for maintaining professional licenses and certifications, as well as protecting the organization’s physical, electronic, and intellectual property assets.
- **Clients and the Marketplace**—This describes commitments and standards around behaving lawfully and ethically and delivering quality service. It also includes other important expectations of conduct, including the importance of maintaining independence and client confidentiality.
- **Public and Community**—This describes the expectation that all employees behave as responsible corporate citizens and the importance of building strong communities with other organizations and charities.

Employee Handbook and Employment Policies

Many organizations also convey expected standards of conduct through corporate policies such as acceptable use policies. The organization may also include these expectations within an employee handbook. In many cases, an organization’s code of conduct and acceptable use policies also apply to vendors or other organizations with which they do business. In fact, in describing the “KPMG Way” from the previous section, KPMG describes its core values as representative of “how our people relate to each other, what we expect of our clients and vendors, and what our clients, vendors, and the marketplace should expect of us.” This also means that IT auditors, who may spend a considerable amount of time at a client organization, not only must represent themselves consistently with their own code, but also must be aware of their client’s expectations.

(ISC)² Code of Ethics

The **International Information Systems Security Certification Consortium (ISC)²** is a nonprofit organization that provides education and certification programs for IS professionals. It develops and maintains a **Common Body of Knowledge (CBK)** that consists of 10 information security domains or high-level topics. The certifications that (ISC)² offers are based on these 10 domains. The (ISC)² certifications are described as follows:

FYI

Those without the years of experience required for (ISC)² certifications may obtain Associate of (ISC)² status. This program is ideal for those switching careers and college students. This achievement requires candidates to pass the CISSP or SSCP certification and adhere to the (ISC)² code of ethics. This program provides various opportunities as benefits. For many, it provides an ideal opportunity to attract potential employers.

- **Systems Security Certified Practitioner (SSCP)**—The **Systems Security Certified Practitioner (SSCP)** is an ideal certification for security engineers, analysts, and administrators. It is also popular for those without primary duties as an IS professional but who would benefit from understanding security. This includes information system auditors, programmers, and database administrators.
- **Certified Authorization Professional (CAP)**—The **Certified Authorization Professional (CAP)** is a certification for managers involved in authorizing and maintaining information systems.
- **Certified Secure Software Lifecycle Professional (CSSLP)**—The **Certified Secure Software Lifecycle Professional (CSSLP)** is a certification for those involved with ensuring security throughout the software life cycle.
- **Certified Information Systems Security Professional (CISSP)**—The **Certified Information Systems Security Professional (CISSP)** is arguably the most recognized information security certification. This certification is ideal for information security management professionals or those who develop policies and procedures for information security. The CISSP includes three concentrations, in architecture, engineering, and management.
- **Certified Cyber Forensics Professional (CCFP)**—The **Certified Cyber Forensics Professional (CCFP)** certification is for those using forensics techniques to support investigations.
- **Healthcare Information Security and Privacy Practitioner (HCISPP)**—The **Healthcare Information Security and Privacy Practitioner (HCISPP)** certification is for information security and privacy professionals who deal with healthcare and patient information.

A goal of (ISC)² is to protect the integrity and value of these certifications as well as the professionalism of the information security industry. As a result, the organization requires credential holders and candidates to adhere to the (ISC)² code of ethics. There are four mandatory principles, or code of ethics canons:

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

The four principles of ethical behavior come with additional guidelines to help resolve ethical dilemmas. The goal is to encourage correct behavior through research, teaching, advancing the profession, and valuing the certifications. The guidelines also discourage certain behaviors. For example, they discourage associating or appearing to associate with criminals or criminal behavior. They also discourage attaching vulnerable systems to the public network, providing unwarranted reassurance, and promoting unnecessary fear, uncertainty, and doubt.

NOTE

Fear, uncertainty, and doubt, or **FUD**, is a common expression within IT circles. FUD is a tactic often seen in politics, sales, and marketing. People use FUD to encourage unfavorable opinions and speculation about a particular topic, often for self-serving interests.

The guiding principles for each requirement are listed on the (ISC)² Web site at <http://www.isc2.org/ethics/default.aspx>. The code of ethics states that complying with these guiding principles is not required, nor does compliance ensure ethical conduct. (ISC)² provides the principles to help members resolve ethical dilemmas they may face during the course of their careers. The (ISC)² board of directors, however, may use the principles to judge the behavior of members.

To protect the reputation of the profession, (ISC)² provides a procedure for ethics complaints. (ISC)² will only consider complaints directly related to one of the four principles. The board of directors established an ethics committee to oversee the process and provide recommendations to the board.

NOTE

Other participants in the Ethics Working Group include the Information Systems Security Association (ISSA) and the Global Information Assurance Certification (GIAC). GIAC is covered later in this chapter.

(ISC)² also participates in the **Ethics Working Group**. The purpose of this group is twofold. First, it defines information security as a recognized profession within IT. Second, it establishes a generally accepted framework of ethical behavior. The Ethics Working Group notes that professions have common characteristics. Having a code of ethics with appropriate oversight is one such characteristic. Others include a common body of knowledge, a governing body, and a certification authority within the profession.

(ISC)² and other member organizations reviewed their respective codes of ethics with the goal of unifying them through the Ethics Working Group. Each organization found many commonalities and consistencies among the various codes. As a result, the group completed the Unified Framework of Professional Ethics for Security Professionals. This framework is organized into four high-level goals, with accompanying details. A summary of the framework is as follows:

- **Integrity**—Act in compliance with laws and apply the highest moral principles.
- **Objectivity**—Act fairly and without prejudice.
- **Professional competence and due care**—Act with professionalism and perform duties diligently.
- **Confidentiality**—Act with respect, protect confidential information, and use due care to prevent inappropriate disclosure.

Certification and Accreditation for IT Auditing

Auditors have an important duty to evaluate organizational controls. These controls affect the confidentiality, integrity, and availability of IT assets and information. As a result, it is vital that IT auditing professionals understand both technology and accounting concepts. In many cases, it's not just desirable but necessary for IT auditing professionals to demonstrate certain levels of competence. If you choose to become certified, you will demonstrate your willingness to improve your knowledge and skills. This provides career benefits as well. It proves your expertise in specific areas to your organization, prospective employer, and

clients.

Certification programs are available that focus solely on IT. Certification programs are also available that focus on auditing. Additionally, certifications exist that blend the two. Such certifications are more aligned to information system auditing and assurance.

Professional certifications have been around for a long time across many different fields. In the IT field, the number of certifications has skyrocketed over the past decade. This is due in part to the many vendor certification programs that are oriented toward specific technologies. These programs are managed by the corresponding vendors, and the programs benefit the vendors from a marketing aspect.

There are also many nonvendor, also called vendor-neutral, certifications. The **Computing Technology Industry Association (CompTIA)** provides one of the oldest nonvendor IT-related certification programs. CompTIA is a nonprofit organization that provides vendor-neutral certification exams. In addition, the organization provides educational programs and market research, and has been involved in activities to advance the IT profession. CompTIA's beginnings go back to 1982. It introduced its first exam, the A+ certification, in 1993. CompTIA was truly a pioneer in the IT security industry. CompTIA certifications include the following:

- **CompTIA A+**—This covers basic operating systems and computer installation, troubleshooting, and communication.
- **CompTIA Network+**—This covers managing and maintaining basic network infrastructure.

FYI

Certification is not the same as licensure. Licensure gives permission to practice within a specific field. Licensure is required for fields that involve a high level of specialization, and that may pose a danger to the individual or the public. Both, however, indicate that an individual has demonstrated a certain level of knowledge or ability. Consider that a license is required to drive a vehicle. Common professions that require licensure include medical practitioners and aviation pilots.

- **CompTIA Security+**—The **CompTIA Security+ certification** covers computer and network security, cryptography, and assessments and audits.
- **CompTIA Server+**—This covers the more advanced computing concepts related to servers.
- **CompTIA Linux+**—This covers the management of Linux operating systems.
- **CompTIA CTT+**—This covers presentation and communication skills for both traditional and virtual class environments.
- **CompTIA CDIA+**—This covers planning and designing of document imaging management systems.
- **CompTIA Project+**—The **CompTIA Project+ certification** covers the process of project management.
- **CompTIA Cloud+**—This covers the topics required to implement and maintain cloud technologies.
- **CompTIA Mobility+**—This covers the management and troubleshooting of mobile devices, including over-the-air technologies.
- **CompTIA Storage+**—This covers storage technologies, including archival, backup, and

retrieval.

- **CompTIA Cloud Essentials**—This covers the secure implementation and maintenance of cloud technologies.
- **CompTIA Healthcare IT Technician**—This covers IT operations as related to the healthcare industry.
- **Social Media Security Professional (SMSP)**—This covers social media skills as related to mitigating security risks.
- **CompTIA IT Fundamentals**—This covers broad IT skills.
- **CompTIA Advanced Security Practitioner (CASP)**—This covers advanced security topics and solutions across complex environments.

Those interested in IT auditing and assessment may find the Project+ and the Security+ certifications especially beneficial. Unlike some of the more advanced certifications discussed in the next section, these certifications are a great starting point. The other certifications that CompTIA offers can also benefit auditing and assessment professionals required to prove knowledge in more specialized areas.

FYI

Most certifications require periodic renewal. Many professional certifications, as part of the renewal process, also require the certification holder to prove continued education. Evidence of continued learning is often in the form of **continuing education units (CEUs)**.

Many certification programs are increasingly seeking **American National Standards Institute (ANSI)** accreditation. ANSI oversees thousands of standards and guidelines across nearly every business sector. ANSI accreditation is based on ISO/IEC international standards to ensure that certification programs are of high quality. ANSI accreditation helps maintain the value of certification programs as ANSI accreditation is recognized as a stamp of approval for a quality certification program.

► NOTE

In 2007, ANSI accredited the CompTIA A+, Network+, and Security+ certifications.

The following sections discuss three well-known and well-respected organizations that offer programs that require a candidate to sufficiently demonstrate competences in the auditing of information systems. A complete list of professional certifications is beyond the scope of this chapter.

IIA

Established in 1941, long before the Internet, when most processes were performed manually, the Institute of Internal Auditors (IIA) is an international professional association for auditors. The IIA's mission is to "provide dynamic leadership for the global profession of internal auditing." To achieve this mission, the IIA supports many activities that promote the value of the internal audit function. Activities include a wide range of educational and developmental opportunities. The IIA is well known for its published standards and guidance

provided to internal auditors.

The IIA provides guidance through the International Professional Practices Framework. This framework includes mandatory and strongly recommended guidance. Mandatory guidance includes the definition of internal auditing, the code of ethics discussed earlier, and various standards. Standards provide the framework for performing internal auditing functions. They include the basic requirements of internal auditing, including further explanations to clarify terms and concepts.

The IIA's recommended guidance includes position papers, practice advisories, and practice guides. The position papers include general topics on governance, risk, and control. They also include explanations of the different roles and responsibilities within the auditing community. The practice advisories assist auditors in applying the standards specific to approaches and methodologies. Finally, the practice guides provide details for internal audit activities. Pertaining to the IT auditor, the IIA provides a series of audit guides specific to IT called **Global Technology Audit Guides (GTAGs)**. These guides provide audit-related guidance pertaining to technology management, control, and security.

FYI

For many years, the IIA provided a Web site and publication named ITAudit. The publication is now called *Internal Auditor* magazine. The Web site is located at <https://iaonline.theiia.org/>. It includes archived issues of ITAudit dating back to 1998.

Another series of guides deals with specific areas related to IT risk and control and is called **Guide to the Assessment of IT Risk (GAIT)**.

In addition, the IIA provides audit-related certifications. These include the following:

- Certified Internal Auditor (CIA)
- Certification in Control Self-Assessment (CCSA)
- Certified Government Auditing Professional (CGAP)
- Certified Financial Services Auditor (CFSAs)
- Certification in Risk Management Assurance (CRMA)

Certified Internal Auditor (CIA) Certification

The **Certified Internal Auditor (CIA)** certification, according to the IIA, is “the only globally accepted certification for internal auditors and remains the standard by which individuals demonstrate their competency and professionalism in the internal auditing field.” The CIA exam covers internal auditing practices and issues, as well as risks and solutions.

The CIA certification is made up of four parts. The first three parts are modeled on the IPPF. A candidate may receive credit for the fourth part if he or she has obtained another related specialty certification. This includes one of the other three IIA certifications or a number of other non-IIA certifications. The Certified Public Accountant (CPA) designation from the American Institute of Certified Public Accountants (AICPA) qualifies, for example. Another example is the Certified Information Systems Auditor (CISA) certification from ISACA, which is explored further in the next section.

The four parts of the CIA exam process are as follows:

- **Part 1**—The Internal Audit Activity’s Role in Governance, Risk, and Control

- **Part 2**—Conducting the Internal Audit Engagement
- **Part 3**—Business Analysis and Information Technology
- **Part 4**—Business Management Skills

To become certified, candidates must meet the following requirements:

- **Exam requirements**—Candidates must complete the exam with a passing score.
- **Educational requirements**—Candidates do not require a bachelor's degree, but having a post-secondary degree will reduce the needed five to seven years of work experience to only two years.
- **Experience requirements**—Candidates with a four-year post secondary degree must have a minimum of two years of experience with internal auditing. Candidates without a degree will require between five and seven years of experience, depending on whether they have any post-secondary education. All experience needs to be verified using a form on the IIA Web site.
- **Professional conduct requirements**—Candidates must abide by the IIA code of ethics. They must also provide a completed IIA character reference form.

The IIA makes exceptions for experience and educational requirements for certain equivalents. In both cases, proper documentation is required.

The following three specialty certifications offered by the IIA also require a bachelor's degree or higher, adherence to the IIA code of conduct, and a completed character reference form.

Certification in Control Self-Assessment (CCSA)

The **Certification in Control Self-Assessment (CCSA)** is for practitioners of **control self-assessments (CSAs)**. A CSA provides a method for those internal to an organization to assess risks and controls on their own. Internal auditors are often involved from a more consultative standpoint and can use the CSA program for focusing audit work on more high-risk areas. Candidates for the CCSA exam must obtain one year of control-related business experience, which could be experience with CSA, auditing, or risk management. The CSA exam covers the following six domains:

- CSA Fundamentals
- CSA Program Integration
- Elements of the CSA Process
- Business Objectives/Organizational Performance
- Risk Identification and Assessment
- Control Theory and Application

Certified Government Auditing Professional (CGAP) Certification

The **Certified Government Auditing Professional (CGAP)** certification is for public sector internal auditors. This exam tests areas of audit knowledge unique to the public sector. This includes grants and legislative oversight. Candidates must obtain two years of auditing experience in a government environment. This can include federal, state, or local government. The CGAP exam covers the following four domains:

- Standards, Governance, and Risk/Control Frameworks

- Government Auditing Practice
- Government Auditing Skills and Techniques
- Government Auditing Environment

Certified Financial Services Auditor (CFSAs) Certification

The **Certified Financial Services Auditor (CFSAs)** exam tests candidate's audit knowledge and abilities with regard to financial services. Candidates must obtain two years of auditing experience in a financial services environment. The exam covers the following four domains:

- Financial Services Auditing
- Auditing Financial Services Products
- Auditing Financial Services Processes
- The Regulatory Environment

In addition to testing on these four domains, the candidate must choose from one of three financial service areas. These include banking, insurance, or securities. The exam includes additional questions specific to the chosen discipline covering the relevant products, processes, and regulatory environments.

Certification in Risk Management Assurance (CRMA) Certification

The **Certification in Risk Management Assurance (CRMA)** exam tests the candidate's ability to evaluate and provide advice on organizational governance and enterprise risk management. CRMA candidates are required to pass [Part 1](#) of the CIA exam and the separate CRMA exam. The CRMA exam covers the following four domains:

- Organizational governance related to risk management
- Principles of risk-management processes
- Assurance role of the internal auditor
- Consulting role of the internal auditor

ISACA

ISACA is a professional association that provides many resources for information systems auditors and IT security and governance professionals. ISACA publishes technical journals, standards, guidelines, and procedures. The organization also promotes research and provides educational programs as well as several professional certifications. ISACA is widely recognized as a result of its popular CISA exam.

ISACA publishes several best-practice framework guidelines. These include COBIT, ITAF, Risk IT, Val IT, and most recently COBIT 5, which combines many of the frameworks into one. In addition, ISACA provides several other educational opportunities and professional resources:

- **Standards**—These are for IT auditors as well as information systems control professionals. The standards provide mandatory requirements for IT audits.
- **Research**—This includes research papers to promote the development of timely topics relevant to IT governance, control, assurance, and security professionals.
- **Publications**—These include the *ISACA Journal*, a bimonthly publication for audit, control, security, and IT governance professionals. Additionally, ISACA offers a

bookstore containing professional development and reference material. There is also an online library, which provides Web access to a wide collection of books.

- **Chapter membership**—This includes membership in chapters around the world that sponsor local education events and seminars and conduct regular meetings.
- **Training and conferences**—These include various conferences that appeal to those new to the field as well as experienced professionals. Additionally, ISACA provides training opportunities such as certification review courses, onsite training, and online courses.
- **Certifications**—These include a handful of certifications for information governance, risk, security, and auditing.

Each ISACA certification requires experience, ethics, education, and an exam. The candidate must pass an exam, adhere to the Code of Professional Ethics, and prove relevant experience. Upon certification, the candidate must also adhere to the continuing professional education program. The continuing education program ensures that certification holders maintain knowledge and skills within the certified area. Each exam is based on a job practice. The job practice provides the foundation for the experience requirements and is the basis of the exam. The job practice is organized by a series of statements that test both knowledge and skills. These are known as task and knowledge statements, which are grouped together and make up parts of the exam, known as domains.

NOTE

ISACA offers its certification exams only twice a year. The exams are available in various cities around the world.

NOTE

Of the ISACA certifications, only the CISA is specifically focused on the IT auditing profession. This does not mean that an IT auditor would not be eligible or benefit from the other certifications. In fact, all the exams cover areas that are relevant to IT auditors.

Certified Information Systems Auditor (CISA) Certification

The **Certified Information Systems Auditor (CISA)** program is well accepted and mature; it's been available since 1978. This certification program is arguably the benchmark for an information systems audit certification for audit, control, and security professionals. In fact, ISACA lists several facts recognizing the significance and importance of the CISA certification. Examples include the following:

- CISA has won or been a finalist in the Best Professional Certification Program from *SC Magazine* for a number of years.
- The National Stock Exchange of India requires CISA certification to conduct system audits.
- CISA is an approved certification for the U.S. Department of Defense Information Assurance Workforce Improvement Program.
- Payment Card Industry Data Security Standard (PCI DSS) accepts CISA as a validation requirement for qualified security assessors.

- The U.S. Federal Reserve Bank requires all assistant examiners to pass the CISA exam before they can be eligible for commissioning.

To qualify, a candidate needs at least five years of professional information systems auditing or security work experience. ISACA provides a list of available substitutions. Candidates may substitute a maximum of one year of information systems experience. Certification holders are also required to adhere to the ISACA information systems auditing standards. CISA covers the following domains:

- **Information Systems Audit Process**—This provides assurance that IT and associated data is protected and controlled. Specifically, this includes making sure that system audit services are within audit standards, guidelines, and best practices.
- **IT Governance**—This provides assurance that a governing program is in place. This includes the structure, policies, processes, and monitoring to achieve effective governance.
- **Systems and Infrastructure Life Cycle Management**—This provides assurance that practices from systems development and acquisition to disposal are adequately in place.
- **IT Service Delivery and Support**—This provides assurance that practices are in place to deliver adequate service levels in line with the business objectives.
- **Protection of Information Assets**—This provides assurance that a security policy framework is in place. This also provides assurance that appropriate controls are in place to protect the confidentiality, integrity, and availability of information systems and data.
- **Business Continuity and Disaster Recovery**—This provides assurance that the business will continue in spite of disruptions.

NOTE

As of 2015, more than 106,000 professionals have earned the CISA designation. ANSI accredits both CISA and CISM.

Certified Information Security Manager (CISM) Certification

The **Certified Information Security Manager (CISM)** certification is designed for information security managers. Candidates also need to prove a minimum of five years of information security experience, which must include three years of experience in three or more of the focus areas or domains. This exam also allows for substitutions. For example, two years may be substituted for a CISA, a CISSP, or a postgraduate degree in information security. CISM covers the following domains:

- Information Security Governance
- Information Risk Management
- Information Security Program Development
- Information Security Program Management
- Incident Management & Response

Certified in Risk and Information Systems Control (CRISC) Certification

Certified in Risk and Information Systems and Control (CRISC) is a broad certification program,

appealing mostly to IT professionals. CRISC tests for knowledge of enterprise risk as well as the life cycle of information systems controls to mitigate risk. Candidates also need to prove at least five years of IT or business experience and at least three years of experience in one or more of the CRISC focus areas. These include the following:

- Risk identification, assessment, and evaluation
- Risk response
- Risk monitoring
- Information systems control design and implementation
- Information systems control monitoring and maintenance

Certified in the Governance of Enterprise IT (CGEIT) Certification

The **Certified in the Governance of Enterprise IT (CGEIT)** certification is targeted to IT governance professionals. This includes those involved in the leadership and processes to help make sure that the IT organization is aligned with an organization's strategies. Candidates need to prove at least five years of experience in a governance support role of an organization's IT department. CGEIT covers the following domains:

- Information Technology Governance Framework
- Strategic Alignment
- Value Delivery
- Risk Management

In addition to ISACA, the SANS Institute, in conjunction with Global Information Assurance Certification, offers IT audit certifications as well as many security-related certifications.

SANS Institute

The **SANS Institute** was founded in 1989 and is a popular source for information security knowledge, training, and certification. Unlike the other organizations, SANS is a for-profit institute and is owned by The Escal Institute of Advanced Technologies.

SANS offers training and certification programs to a wide range of IT professionals. The training spans different groups, such as audit, network, and security, as well as positions from system administrators to chief information security officers (CISOs).

In addition, SANS provides a variety of free resources, including a large collection of documents in its Reading Room, found online. The Reading Room features computer security technical papers in dozens of categories.

SANS offers a wide selection of training programs and a variety of delivery methods. These include the following:

- **Classroom training events**—These are offered many times throughout the year across major cities globally. These SANS events are similar to professional conferences in that they also offer networking opportunities, vendor product information, and guest speakers.
- **SANS WhatWorks Summits**—These unique two-day events provide information on current topics in computer security.
- **Community training events**—The community events provide the same content as the classroom events, but in small classroom settings within local communities.

- **Mentor sessions**—Mentor sessions provide a multiweek program to learn from an assigned mentor the same material offered in the classroom training and community training events.
- **Onsite training**—Training can be provided at your workplace. This is ideal for organizations that would like to train a large number of personnel.
- **Partnership series**—This series provides discounted training to specific groups where classes will be more than 125 people. These groups include, for example, those whose work affects national security or groups that have budget constraints.
- **SANS vLive!**—This program provides live instructor-led training over the Web.
- **SANS OnDemand**—This program provides training similar to SANS vLive over the Web, but not in a live environment. Rather, it includes on-demand integrated courseware.
- **Self study**—Similar to SANS OnDemand, self study is more focused on certification study. This program provides the learner with printed course books, CDs, and practice questions.

In 1999, SANS established the **Global Information Assurance Certification (GIAC)**. GIAC operates as a separate entity, although like SANS, it is a trademark name of The Escal Institute of Advanced Technologies. GIAC provides many different vendor-neutral information security certifications. These certifications are grouped within four different tracks:

- IT audit
- Security administration
- Security management
- Software security

GIAC Certifications

GIAC certifications include those listed in [Table 15-1](#). After attaining one of these certifications, the certification holder can achieve Gold certification or Expert Level certification by demonstrating a deeper level of knowledge. The GIAC Gold program requires the candidate to work with an assigned advisor while writing a detailed technical report. These papers are subsequently published by SANS in the Reading Room. The GIAC Expert Level certification program involves a multiday experience in which the candidate must complete individual- and group-based exercises. This includes, for example, presentations, research, essays, and hands-on testing exams.

NOTE

There were two other auditrelated GIAC certifications, named GIAC Security Audit Essentials (GSAE) and GIAC Certified ISO-27000 Specialist. These exams have been retired and are no longer available.

Of the many different exams, GIAC provides one exam focused on IT auditing: the GSNA. All the GIAC certifications are tied to specific SANS training courses. SANS training, however, is not required. Experienced candidates have the option to instead purchase a GIAC Exam Challenge. This includes access to two practice tests and the certification exam.

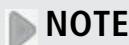
TABLE 15-1 GIAC certification programs.

LEVEL	CERTIFICATION	DESIGNATION	TRACK
Introductory	GIAC Information Security Fundamentals	GISF	Security Administration
	GIAC Security Essentials Certification	GSEC	Security Administration
Intermediate	GIAC Industrial Cyber Security Professional	GISCP	Management
	GIAC Certified Forensics Examiner	GCFE	Forensics
	GIAC Mobile Device Security Analyst	GMOB	Security Administration
Advanced	GIAC Critical Controls Certification	GCCC	Audit
	GIAC Certified Perimeter Protection Analyst	GPPA	Security Administration
	GIAC Certified Intrusion Analyst	GCIA	Security Administration
	GIAC Certified Incident Handler	GCIH	Security Administration
	GIAC Certified UNIX Security Administrator	GCUX	Security Administration
	GIAC Certified Windows Security Administrator	GCWN	Security Administration
	GIAC Certified Enterprise Defender	GCED	Security Administration
	GIAC Certified Penetration Tester	GPEN	Security Administration
	GIAC Web Application Penetration Tester	GWAPT	Security Administration
	GIAC Security Leadership Certification	GSLC	Management
	GIAC Certified Project Manager Certification	GCPM	Management
	GIAC Secure Software Programmer-.NET	GSSP-NET	Software Security
	Secure Software Programmer-Java	GSSP-JAVA	Software Security
	GIAC Systems and Network Auditor	GSNA	Audit
	GIAC Certified Forensic Analyst	GCFA	Forensics
	GIAC Law of Data Security & Investigations	GLEG	Legal
Expert	GIAC Assessing and Auditing Wireless Networks	GAWN	Security Administration
	GIAC Exploit Researcher and Advanced Penetration Tester	GXPN	Security Administration
	GIAC Reverse Engineering Malware	GREM	Forensics
	GIAC Security Expert	GSE	GSE

GIAC Systems and Network Auditor (GSNA) Certification

The **GIAC Systems and Network Auditor (GSNA)** certification assesses the candidate's understanding of more than three dozen exam certification objectives. The following is an abridged list of these objectives and expectations:

- Understand basic auditing terms as well as strategies for baseline security controls.
- Understand defense in depth as it applies to critical systems and methods to audit them.
- Identify perimeter systems and firewall architecture as well as plan and manage a perimeter audit.
- Understand how a risk assessment is used to identify necessary controls.
- Describe the auditing process from planning to the final report to management.
- Understand the concepts of auditing databases and understanding SQL basics.
- Understand router configurations and access controls lists as well as secure switch architecture.
- Demonstrate basic operating system knowledge of UNIX and Windows systems, including audit, logging, and security fundamentals.
- Understand the tools and methodologies for conducting a vulnerability assessment.
- Understand how to identify and audit wireless devices and modems.
- Understand various aspects of Web technology, including Web applications and Web vulnerabilities and security.



NOTE

Both the CISA and the GSNA demonstrate competencies with regard to IT and auditing. The CISA, however, tends to be more audit focused, while the GSNA is more technically focused.

SANS continued its growth in 2008 with the introduction of the SANS Technology Institute. The institute provides graduate-level educational programs, which grant master's degrees in information security. The SANS Technology Institute has been authorized by the Maryland Higher Education Commission to grant such a degree. In 2013, the SANS Technology Institute gained regional accreditation by the Middle States Commission on Higher Education.

Admission into the institute requires successful completion of undergraduate work as well as additional requirements related to information security. This includes professional experience in the field. In addition, candidates must hold a major GIAC Gold certification.



CHAPTER SUMMARY

The IT audit profession continues to grow and is supported by several professional organizations. IT auditors need to strongly adhere to ethical codes and be in constant pursuit of continued education. There are numerous educational opportunities for those just entering the profession and those looking for growth. Organizations such as the IIA and ISACA provide a tremendous amount of resources for the profession. Practitioners within the audit field, the IT field, or a combination of both should strongly consider membership and take advantage of the educational and certification opportunities.



KEY CONCEPTS AND TERMS

American National Standards Institute (ANSI)
Certified Authorization Professional (CAP)
Certification in Control Self-Assessment (CCSA)
Certified Cyber Forensics Professional (CCFP)
Certified Financial Services Auditor (CFSA)
Certified Government Auditing Professional (CGAP)
Certified in Risk and Information Systems and Control (CRISC)
Certification in Risk Management Assurance (CRMA)
Certified in the Governance of Enterprise IT (CGEIT)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
Certified Information Systems Security Professional (CISSP)
Certified Internal Auditor (CIA)
Certified public accountants (CPAs)
Certified Secure Software Lifecycle Professional (CSSLP)
Code of conduct
Code of ethics
Common Body of Knowledge (CBK)
CompTIA Project+ certification
CompTIA Security+ certification
Computing Technology Industry Association (CompTIA)
Continuing education units (CEUs)
Control self-assessments (CSAs)
Due care
Ethics
Ethics Working Group
FUD
GIAC Systems and Network Auditor (GSNA)
Global Information Assurance Certification (GIAC)
Global Technology Audit Guides (GTAGs)
Guide to the Assessment of IT Risk (GAIT)
Healthcare Information Security and Privacy Practitioner (HCISPP)
Institute of Internal Auditors (IIA)
International Information Systems Security Certification Consortium (ISC)²
International Professional Practices Framework (IPPF)
SANS Institute
SANS Technology Institute
Systems Security Certified Practitioner (SSCP)



CHAPTER 15 ASSESSMENT

1. Which of the following is *not* considered a soft skill needed by IT auditors?

 - A. Penetration testing skills
 - B. Negotiation skills
 - C. Business writing skills
 - D. Behavior skills
 - E. Communication skills
 - F. Leadership skills
2. A(n) _____ of ethics for IT auditors is important for outlining clear ethical expectations.
3. The Sarbanes-Oxley Act does *not* attempt to define a code of ethics, but rather it references the code of ethics established by the IIA.

 - A. True
 - B. False
4. According to IFAC, the rules of behavior that guide the decisions of an organization should do which of the following? (Select the two best answers.)

 - A. Contribute to the personal fortunes of IT vendors.
 - B. Contribute to the welfare of key stakeholders.
 - C. Respect the rights of all constituents affected by the organization's operations.
 - D. Consider what is best for the organization's stock price.
 - E. Respect that each individual has a different moral code.
5. A thorough code of conduct would include which of the following?

 - A. The company's mission
 - B. The company's values
 - C. Examples of ethical and unethical behavior
 - D. All of the above
6. The NYSE requires that companies listed on its exchange publicly make available a code of conduct.

 - A. True
 - B. False
7. An individual holding which of the following certifications should be familiar with the (ISC)² code of ethics?

 - A. SSCP
 - B. CISA
 - C. CISSP
 - D. Answers A and C
 - E. None of the above
8. Which of the following is *not* a mandatory principle or canon of the (ISC)² code of ethics?

 - A. Protect society, the commonwealth, and the infrastructure.
 - B. Act honorably, honestly, justly, responsibly, and legally.
 - C. Provide diligent and competent service to principals.
 - D. Advance and protect the profession.
 - E. Serve justly, competently, and with pretense.
9. Certification and licensure are essentially the same thing.

 - A. True
 - B. False
10. Which of the following organizations provides IT-related professional certifications?

 - A. CompTIA
 - B. ISACA
 - C. ANSI
 - D. All of the above

E. Answers A and B only

- 11.** Which of the following is *not* professional guidance provided by the IIA?
- A. COBIT
 - B. GAIT
 - C. GTAG
 - D. IPPF
- 12.** A candidate for the Certified Internal Auditor certification must first achieve the Certified Information Systems Auditor certification.
- A. True
 - B. False
- 13.** To become an ISACA Certified Information Systems Auditor, which of the following is required?
- A. Successfully pass an examination
 - B. Adhere to an ethical code
 - C. Experience
 - D. All of the above
- 14.** The SANS Institute is a nonprofit organization that provides free certification exams across four different information security tracks.
- A. True
 - B. False
- 15.** Which of the following is a GIAC certification that would most likely appeal to an IT auditor?
- A. GSNA
 - B. GLEG
 - C. GCFA
 - D. CISSP
 - E. CISA

¹. Reprinted with the permission of ISACA, from “Code of Professional Ethics” by ISACA.

APPENDIX A

Answer Key

CHAPTER 1 The Need for Information Systems Security Compliance

1. B
2. Risk-based approach
3. A
4. A guide for assessing security controls
5. D
6. B
7. Independent
8. C
9. A
10. D
11. E
12. E
13. D
14. E
15. Strict liability

CHAPTER 2 Overview of U.S. Compliance Laws

1. A
2. C
3. Risk
4. A
5. B
6. B
7. C
8. E
9. D
10. A
11. B
12. C
13. B
14. B
15. E

CHAPTER 3 What Is the Scope of an IT Compliance Audit?

1. Gap
2. C
3. A
4. A
5. B

- 6. C
- 7. E
- 8. B
- 9. D
- 10. Framework
- 11. D
- 12. A, B, and C
- 13. A, B, and E
- 14. Identity

CHAPTER 4 Auditing Standards and Frameworks

- 1. Framework
- 2. A
- 3. B
- 4. A, B, and C
- 5. A
- 6. B
- 7. Goal
- 8. B
- 9. B
- 10. B
- 11. B
- 12. Practice
- 13. D
- 14. C

CHAPTER 5 Planning an IT Infrastructure Audit for Compliance

- 1. E
- 2. C
- 3. B
- 4. Threat
- 5. C
- 6. A
- 7. D
- 8. Scope
- 9. A
- 10. A
- 11. E
- 12. B
- 13. A
- 14. C
- 15. D

CHAPTER 6 Conducting an IT Infrastructure Audit for Compliance

- 1. A
- 2. C
- 3. B
- 4. B
- 5. Penetration test

6. A
7. A
8. A
9. D
10. A
11. Management
12. A
13. A
14. A
15. C

CHAPTER 7 Writing the IT Infrastructure Audit Report

1. A
2. B
3. B
4. B
5. A
6. B
7. A
8. C
9. A
10. A

CHAPTER 8 Compliance Within the User Domain

1. B
2. Business drivers
3. C
4. A
5. Need to know
6. B
7. D
8. B
9. C
10. A
11. C
12. B
13. C
14. B
15. A

CHAPTER 9 Compliance Within the Workstation Domain

1. Due diligence
2. B
3. B and C
4. War dialing
5. A
6. B
7. C
8. C

- 9. A
- 10. Integrity
- 11. A and D
- 12. Worm

CHAPTER 10 Compliance Within the LAN Domain

- 1. B
- 2. B
- 3. B
- 4. Fiber optic
- 5. A
- 6. A
- 7. C
- 8. B
- 9. Network monitoring platform, or NMP
- 10. C
- 11. A
- 12. Availability
- 13. B and C
- 14. B
- 15. C

CHAPTER 11 Compliance Within the LAN-to-WAN Domain

- 1. A
- 2. A
- 3. Proxy server
- 4. Demilitarized zone (DMZ)
- 5. B
- 6. Single point of failure
- 7. B and C
- 8. C
- 9. A
- 10. C
- 11. Virtual private network (VPN)
- 12. B
- 13. A
- 14. Multi-Protocol Label Switching (MPLS)
- 15. A

CHAPTER 12 Compliance Within the WAN Domain

- 1. B
- 2. A
- 3. B
- 4. C
- 5. A
- 6. Service level agreement (SLA)
- 7. A
- 8. C
- 9. WAN optimizer

- 10. B
- 11. B
- 12. C
- 13. Virtual private network, or VPN
- 14. D

CHAPTER 13 Compliance Within the Remote Access Domain

- 1. B
- 2. C
- 3. Encryption
- 4. B
- 5. A
- 6. D
- 7. A
- 8. Tunneling
- 9. B
- 10. B
- 11. SNMP
- 12. A
- 13. D
- 14. B
- 15. B

CHAPTER 14 Compliance Within the System/Application Domain

- 1. B
- 2. B
- 3. A
- 4. Subnet
- 5. C
- 6. People
- 7. B
- 8. C
- 9. C
- 10. Web server
- 11. A
- 12. A and C
- 13. B

CHAPTER 15 Ethics, Education, and Certification for IT Auditors

- 1. A
- 2. Code
- 3. B
- 4. B and C
- 5. D
- 6. A
- 7. D
- 8. E
- 9. B
- 10. E

11. A

12. A

13. D

14. B

15. A

APPENDIX B

Standard Acronyms

ACD	automatic call distributor
AES	Advanced Encryption Standard
ALE	annual loss expectancy
ANSI	American National Standards Institute
AO	authorizing official
AP	access point
API	application programming interface
APT	advanced persistent threat
ARO	annual rate of occurrence
ATM	asynchronous transfer mode
AUP	acceptable use policy
AV	antivirus
B2B	business to business
B2C	business to consumer
BBB	Better Business Bureau
BC	business continuity
BCP	business continuity plan
BGP4	Border Gateway Protocol 4 for IPv4
BIA	business impact analysis
BYOD	Bring Your Own Device
C2C	consumer to consumer
CA	certificate authority
CAC	Common Access Card
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act
CAP	Certification and Accreditation Professional
CAUCE	Coalition Against Unsolicited Commercial Email
CBA	cost-benefit analysis
CBF	critical business function
CBK	common body of knowledge
CCC	CERT Coordination Center
CCNA	Cisco Certified Network Associate
CDR	call-detail recording
CERT	Computer Emergency Response Team
CFE	Certified Fraud Examiner
C-I-A	confidentiality, integrity, availability
CIPA	Children's Internet Protection Act
CIR	committed information rate
CIRT	computer incident response team
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information System Security Professional
CMIP	Common Management Information Protocol

CMMI	Capability Maturity Model Integration
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
COPPA	Children's Online Privacy Protection Act
COS	class of service
CRC	cyclic redundancy check
CSA	Cloud Security Alliance
CSF	critical success factor
CSI	Computer Security Institute
CSP	cloud service provider
CTI	Computer Telephony Integration
CVE	Common Vulnerabilities and Exposures
DAC	discretionary access control
DBMS	database management system
DCS	distributed control system
DDoS	distributed denial of service
DEP	data execution prevention
DES	Data Encryption Standard
DHCPv6	Dynamic Host Configuration Protocol v6 for IPv6
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DISA	direct inward system access
DMZ	demilitarized zone
DNS	Domain Name Service OR Domain Name System
DoD	Department of Defense
DoS	denial of service
DPI	deep packet inspection
DR	disaster recovery
DRP	disaster recovery plan
DSL	digital subscriber line
DSS	Digital Signature Standard
DSU	data service unit
EDI	Electronic Data Interchange
EIDE	Enhanced IDE
ELINT	electronic intelligence
EPHI	electronic protected health information
EULA	End-User License Agreement
FACTA	Fair and Accurate Credit Transactions Act
FAR	false acceptance rate
FCC	Federal Communications Commission
FDIC	Federal Deposit Insurance Corporation
FEP	front-end processor
FERPA	Family Educational Rights and Privacy Act
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FRCP	Federal Rules of Civil Procedure
FRR	false rejection rate
FTC	Federal Trade Commission
FTP	File Transfer Protocol
GAAP	generally accepted accounting principles

GIAC	Global Information Assurance Certification
GigE	Gigabit Ethernet LAN
GLBA	Gramm-Leach-Bliley Act
HIDS	host-based intrusion detection system
HIPAA	Health Insurance Portability and Accountability Act
HIPS	host-based intrusion prevention system
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HUMINT	human intelligence
IaaS	Infrastructure as a Service
IAB	Internet Activities Board
ICMP	Internet Control Message Protocol
IDEA	International Data Encryption Algorithm
IDPS	intrusion detection and prevention
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IMINT	imagery intelligence
InfoSec	information security
IP	intellectual property OR Internet Protocol
IPS	intrusion prevention system
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS-IS	intermediate system-to-intermediate system
(ISC)²	International Information System Security Certification Consortium
ISO	International Organization for Standardization
ISP	Internet service provider
ISS	Internet security systems
ITIL	Information Technology Infrastructure Library
ITRC	Identity Theft Resource Center
IVR	interactive voice response
L2TP	Layer 2 Tunneling Protocol
LAN	local area network
MAC	mandatory access control
MAN	metropolitan area network
MAO	maximum acceptable outage
MASINT	measurement and signals intelligence
MD5	Message Digest 5
modem	modulator demodulator
MP-BGP	Multiprotocol Border Gateway Protocol for IPv6
MPLS	multiprotocol label switching
MSTI	Multiple spanning tree instance
MSTP	Multiple Spanning Tree Protocol
NAC	network access control
NAT	network address translation
NFIC	National Fraud Information Center
NIC	network interface card

NIDS	network intrusion detection system
NIPS	network intrusion prevention system
NIST	National Institute of Standards and Technology
NMS	network management system
NOC	network operations center
NSA	National Security Agency
NVD	national vulnerability database
OPSEC	operations security
OS	operating system
OSI	Open Systems Interconnection
OSINT	open source intelligence
OSPFv2	Open Shortest Path First v2 for IPv4
OSPFv3	Open Shortest Path First v3 for IPv6
PaaS	Platform as a Service
PBX	private branch exchange
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PGP	Pretty Good Privacy
PII	personally identifiable information
PIN	personal identification number
PKI	public key infrastructure
PLC	programmable logic controller
POAM	plan of action and milestones
PoE	power over Ethernet
POS	point-of-sale
PPTP	Point-to-Point Tunneling Protocol
PSYOPS	psychological operations
RA	registration authority OR risk assessment
RAID	redundant array of independent disks
RAT	remote access Trojan OR remote access tool
RFC	Request for Comments
RIPng	Routing Information Protocol next generation for IPv6
RIPv2	Routing Information Protocol v2 for IPv4
ROI	return on investment
RPO	recovery point objective
RSA	Rivest, Shamir, and Adleman (algorithm)
RSTP	Rapid Spanning Tree Protocol
RTO	recovery time objective
SA	security association
SaaS	Software as a Service
SAN	storage area network
SANCP	Security Analyst Network Connection Profiler
SANS	SysAdmin, Audit, Network, Security
SAP	service access point
SCADA	supervisory control and data acquisition
SCSI	small computer system interface
SDSL	symmetric digital subscriber line
SET	secure electronic transaction
SGC	server-gated cryptography
SHA	secure hash algorithm
S-HTTP	secure HTTP

SIEM	Security Information and Event Management system
SIGINT	signals intelligence
SIP	Session Initiation Protocol
SLA	service level agreement
SLE	single loss expectancy
SMFA	specific management functional area
SNMP	Simple Network Management Protocol
SOX	Sarbanes-Oxley Act of 2002 (also Sarbox)
SPOF	single point of failure
SQL	Structured Query Language
SSA	Social Security Administration
SSCP	Systems Security Certified Practitioner
SSID	service set identifier (name assigned to a Wi-Fi network)
SSL	Secure Sockets Layer
SSL-VPN	Secure Sockets Layer virtual private network
SSO	single system sign-on
STP	shielded twisted pair OR Spanning Tree Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TFA	two-factor authentication
TFTP	Trivial File Transfer Protocol
TGAR	trunk group access restriction
TNI	Trusted Network Interpretation
TPM	technology protection measure OR trusted platform module
UC	unified communications
UDP	User Datagram Protocol
UPS	uninterruptible power supply
USB	universal serial bus
UTP	unshielded twisted pair
VA	vulnerability assessment
VBAC	view-based access control
VLAN	virtual local area network
VoIP	Voice over Internet Protocol
VPN	virtual private network
W3C	World Wide Web Consortium
WAN	wide area network
WAP	wireless access point
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	wireless local area network
WNIC	wireless network interface card
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
XML	Extensible Markup Language
XSS	cross-site scripting

Glossary of Key Terms

10 U.S. Code Section 2223, Information Technology: Additional Responsibilities of Chief Information Officers | A United States code that provides the basis for assigning responsibilities, functions, relationships, and authorities to the Department of Defense (DoD) Chief Information Officer (CIO).

10 U.S. Code Section 2224, Defense Information Assurance Program | A United States code that provides guidance for creating an information advantage for the Department of Defense (DoD).

A

Acceptable use policy (AUP) | A policy that defines which actions are acceptable and which ones aren't.

Access control lists (ACLs) | Lists of permissions that define which users or groups can access an object.

Acts of Congress | Statutes or public laws enacted by Congress.

American National Standards Institute (ANSI) | A nonprofit accrediting organization that oversees the development of standards.

Application performance monitoring software | Software that can measure end-user response time for application software server requests as well as end-user traffic volume.

Approved Scanning Vendor (ASV) | A qualified and approved company able to perform Payment Card Industry (PCI) vulnerability scans and assessments.

Assurance | A level of confidence that appropriate and effective IT controls are in place.

Audit | An independent assessment that takes a well-defined approach to examining an organization's internal policies, controls, and activities.

Audit frequency | The rate of occurrence for an audit.

Audit objective | The goal of an audit.

Audit scope | The range of the organization to be included in an audit within a defined time frame.

Auditing Standard No. 5 | An audit of internal control of financial reporting that is integrated with an audit of financial statements.

Authentication | The process of providing additional credentials that match the user ID or user name.

Authorization | The process of granting rights and permissions to access objects to a subject.

Availability | The assurance that information is available to authorized users in an acceptable time frame when the information is requested.

B

Background check | An investigation to divulge evidence of past behavior that may indicate that a prospect is a security risk.

Baseband | A transmission technique that uses the entire channel's bandwidth.

Baseline | A system in a known good state, with the minimum controls relative to the accepted risk applied.

Baseline controls | Countermeasures that apply broadly to the entire IT infrastructure.

Broadband | A transmission technique that uses only a portion of the full bandwidth of a channel.

Business continuity plans (BCPs) | Plans that document the steps to restore business operation after an interruption. BCPs, along with DRPs, enable you to recover from disruptions ranging from small to large.

Business drivers | The components, including people, information, and conditions, that support business objectives.

Card verification value (CVV) | A number printed on a credit card that provides additional authentication when rendering payment for online transactions.

Certification and accreditation (C&A) | An audit of a federal system before being placed into a production environment.

Certification in Control Self-Assessment (CCSA) | An IIA certification that tests professional knowledge of control self-assessments.

Certified Authorization Professional (CAP) | An (ISC)² certification that tests a candidate's knowledge of the process of certifying and accrediting the security of information systems.

Certified Cyber Forensics Professional (CCFP) | A certification for those using forensics techniques to support investigations.

Certified Financial Services Auditor (CFSAs) | An IIA certification that tests one's knowledge and abilities of audits pertaining to financial services.

Certified Government Auditing Professional (CGAP) | An IIA certification that tests audit knowledge unique to the public sector.

Certified in Risk and Information Systems and Control (CRISC) | An ISACA certification that tests knowledge of enterprise risk and control.

Certified in the Governance of Enterprise IT (CGEIT) | An ISACA certification that tests knowledge of IT governance concepts.

Certified Information Security Manager (CISM) | An ISACA certification that tests required knowledge of information security managers.

Certified Information Systems Auditor (CISA) | An ISACA certification exam considered by many to be the gold standard for IT auditing.

Certified Information Systems Security Professional (CISSP) | An (ISC)² certification considered by many to be the gold standard for information security management.

Certified Internal Auditor (CIA) | An IIA certification exam that covers internal auditing practices and issues.

Certified public accountants (CPAs) | A designation earned by qualified accountants in the United States after passing an accounting certification exam and meeting other professional requirements.

Certified Secure Software Lifecycle Professional (CSSLP) | An (ISC)² certification that tests candidates on IT security throughout the software life cycle.

Chief privacy officer (CPO) | A senior-level position responsible for the overall management of an organization's privacy program.

Children's Internet Protection Act (CIPA) | An act of Congress to address concerns about minors' access to explicit online content.

Children's Online Privacy Protection Act (COPPA) | A United States federal law designed with the intent to protect children. COPPA is maintained and enforced by the FTC. COPPA requires Web sites and other online services aimed at children less than 13 years of age to comply with specific requirements of the law.

C-I-A | The confidentiality, integrity, and availability (C-I-A) properties that describe a secure object. Also referred to as availability, integrity, and confidentiality (A-I-C).

Ciphertext | The unreadable output that results from encryption. Encryption turns cleartext data into ciphertext through the use of an algorithm and a key.

Cleartext | Human-readable data.

Clinger-Cohen Act of 1996 | A United States law that improves upon the acquisition, use, and disposal of federal IT resources.

Code of conduct | A statement of procedures and guiding principles to influence the culture and behavior

of an organization's employees.

Code of ethics | A statement of general principles that pertain to an organization and its constituents.

Committee of Sponsoring Organizations (COSO) of the Treadway Commission | An organization that provides guidance to executive management on organizational governance, internal controls, and risk management.

Common Body of Knowledge (CBK) | An (ISC)² term that describes the 10 topics that form the knowledge areas of its members.

Compensating controls | Alternative counter-measures to minimize risk.

Compliance | The act of adhering to internal policies, applicable laws, regulations, and industry requirements.

CompTIA Project+ certification | A CompTIA certification that tests knowledge of project management.

CompTIA Security+ certification | A CompTIA certification that tests basic IT security concepts.

Computer assisted audit tools and techniques (CAATT) | Automated computerized tools and techniques that auditors use to aid them in their auditing function.

Computing Technology Industry Association (CompTIA) | A nonprofit professional association known for its many certifications covering a wide range of topics.

Confidentiality | Assurance that information is not disclosed to unauthorized sources.

Confidentiality agreement | A legally binding document in which the parties agree that certain types of information will pass among the parties and must remain confidential and not divulged. Also commonly called a non-disclosure agreement (NDA).

Configuration and change management | The detailed recording, management, and updating of the details of an information system.

Configuration control board (CCB) | A person or group of people who reviews each change request and approves or denies the request.

Configuration management database (CMDB) | A central repository of system configuration items.

Connection media | The adapters and wires or wireless media that connect components together in the LAN Domain.

Consensus Audit Guidelines (CAG) | A listing of the top 20 critical security controls, published by SANS.

Continuing education units (CEUs) | Measurements used in continuing education programs such as certifications.

Control activities | Activities that provide the details on how to achieve control objectives.

Control objectives | Objectives that state the high-level organizational goals of information system measures.

Control Objectives for Information and Related Technology (COBIT) | A framework that provides best practices for IT governance and control.

Control self-assessments (CSAs) | Methods for organizations to assess risk and controls on their own.

Controls | Actions or changes put in place to reduce a weakness or potential loss. A control is also referred to as a countermeasure.

Corrective controls | Mechanisms that repair damage caused by an undesired action and limit further damage, such as the procedure to remove detected viruses or the use of a firewall to block an attacking system.

Critical Security Controls | A list of 20 security controls primarily addressing the technical control area.

Cybersecurity | The practice of protecting computers and electronic communication systems as well as the associated information.

Cybersecurity Framework | Developed by NIST, a framework that provides a voluntary structure for reducing the risks to critical infrastructure.

Data center | One or more rooms with protected access and a controlled environment for computers and other IT devices. Also called a computer room.

Data leak security appliances | Network devices or software running on computers that scan network traffic for data-matching rules.

Dedicated line | A permanent circuit between two endpoints.

Demilitarized zone (DMZ) | A separate network or portion of a network that is connected to a WAN and at least one LAN, with at least one firewall between the DMZ and the LAN.

Denial of service (DoS) | An attack that generally floods a network with traffic. A successful DoS attack renders the network unusable and effectively stops the victim organization's ability to conduct business.

Descriptive control | A measure to be applied to a system that is high level and provides a lot of flexibility.

Detective controls | Mechanisms that recognize when an undesired action has occurred, such as motion detectors or usage log analysis tools.

Digital certificates | Cryptography-related electronic documents that allow for node identification and authentication. Digital certificates require more administrative work than some other methods but provide greater security.

Disaster recovery plans (DRPs) | Plans that document the steps you can take to replace damaged or destroyed components due to a disaster to restore the integrity of your IT infrastructure. DRPs, along with BCPs, enable you to recover from disruptions ranging from small to large.

Discretionary access control (DAC) | An access permission based on roles or groups that allows object owners and administrators to grant access rights at their discretion.

Distributed applications | Applications whose components reside on different computers.

Dual-homed ISP connection | A design in which a network maintains two connections to its ISP.

Due care | The level of effort IT security professionals owe their employers and colleagues.

Due diligence | Reasonable steps taken to ensure adherence to requirements.

E

E-Government Act of 2002 | A United States law that improves the management of electronic government services by establishing a framework that requires the use of the Internet and related technologies to improve citizen access to government information services.

Encapsulating protocol | A protocol that encrypts each message for transport by a nonencrypting protocol.

Encryption | The process of scrambling data in such a way that it is unreadable by unauthorized users but can be unscrambled by authorized users to be readable again.

Enron | A large U.S.-based energy company that went bankrupt in 2001 and has become a symbol of corporate fraud and corruption.

Enterprise risk management (ERM) | The governing process for managing risks and opportunities.

Enterprise risk management (ERM) framework | The process organizations use to manage risks related to achieving their goals.

Ethernet | A widely used LAN protocol for connecting a network. It is inexpensive to deploy and provides substantial bandwidth for the low cost.

Ethernet MAN | A hybrid network that uses Ethernet on a Metro Ethernet, or MAN.

Ethics | Moral beliefs and rules with regard to what is right and wrong.

Ethics Working Group | A consortium to define information security as a recognized profession within IT and to establish a generally accepted framework of ethical behavior.

Executive summary | A concise yet informative review intended for senior level management or those with decision-making power.

F

Fair Credit Reporting Act (FCRA) | U.S. legislation that defines national standards for all consumer reports.

Family Educational Rights and Privacy Act (FERPA) | An act of Congress to protect the privacy of education records.

FCAPS | The acronym for a network management functional model that stands for fault, configuration, accounting, performance, and security.

Federal Information Processing Standards (FIPS) | Technical standards published by NIST and approved by the Secretary of Commerce.

Federal Information Security Management Act of 2002 (FISMA) | An act of Congress to recognize the importance of information security to the interests of the United States.

Finding | A documented conclusion that highlights deficiencies, abuse, fraud, or other questionable acts.

Fingerprinting | The process of identifying the operating system and general configuration of a computer.

Firewall | A network security measure designed to filter out undesirable network traffic.

Footprinting | The process of determining the operating system and version of a network node.

Framework | A conceptual set of rules and ideas that provide structure to a complex and challenging situation.

FUD | An acronym used to describe fear, uncertainty, and doubt.

G

Gap analysis | A comparison between the actual outcome and the desired outcome.

Generally Accepted Privacy Principles (GAPP) | A set of principles developed to provide guidance for privacy audits.

GIAC Systems and Network Auditor (GSNA) | A GIAC certification that tests technically focused knowledge of information systems auditing.

Global Information Assurance Certification (GIAC) | A SANS-associated organization that provides an assortment of information assurance certifications.

Global Technology Audit Guides (GTAGs) | IIA-published documents that provide audit guidance for IT auditors.

Governance | The process through which an organization's processes and assets are directed and controlled.

Gramm-Leach-Bliley Act (GLBA) | An act of Congress to protect the financial aspects of consumer information held by financial agencies.

Guide to the Assessment of IT Risk (GAIT) | IIA-published documents that provide guidance related to IT risk and control.

Guideline | A document that supports standards and policies, but is not mandatory.

H

Halon | A gas commonly used in data center fire-suppression systems. Due to halon's toxic properties, one type of halon has been banned and is no longer produced. Alternative gases are becoming more common.

Healthcare Information Security and Privacy Practitioner (HCISPP) | A certification for information security and privacy professionals who deal with healthcare and patient information.

Health Information Technology for Economic and Clinical Health Act (HITECH) | An act of Congress that builds on HIPAA by providing for increased enforcement and breach notification.

Health Insurance Portability and Accountability Act (HIPAA) | An act of Congress that helps citizens maintain their health coverage as well as improve the efficiency and effectiveness of the American

healthcare system.

Honeypot | A server deliberately set up to be unsecure in an effort to trap or track attackers.

Hub | A box with several connectors, or ports, that allows multiple network cables to attach to it. A hub is basically a hardware repeater. It takes input from any port and repeats the transmission, sending it as output on every port, including the original port.

Hypertext Transfer Protocol (HTTP) | An Application Layer protocol most commonly associated with the Web.

Hypertext Transfer Protocol Secure (HTTPS) | A more secure version of HTTP.

I

Identification | The process of providing user credentials or claiming to be a specific user.

Identity theft | The taking of one's personal information for unauthorized use.

IEEE 802.11 | A group of standards for WLAN communication protocols.

Information resource management | A process of managing information to improve performance.

Information security management system (ISMS) | The policies, standards, and programs related to information security.

Information Systems Security Assessment Framework (ISSAF) | A method for evaluating networks, systems, and applications.

Information Technology Assurance Framework (ITAF) | A framework for IT assurance, created by ISACA.

Information Technology Governance Institute (ITGI) | A research think tank that provides resources on IT governance.

Information Technology Laboratory (ITL) Bulletins | NIST publications that provide in-depth coverage of important topics.

Institute of Electrical and Electronics Engineers (IEEE) | An organization that defines standards for many aspects of computing and communications.

Institute of Internal Auditors (IIA) | A professional body for internal audit professionals that offers guidance on relevant topics.

Integrated audit | An audit that combines the assessment of financial reporting with the assessment of related IT controls.

Integrity | Assurance against unauthorized modification or destruction.

Intellectual property rights (IPRs) | The exclusive privilege to intangible assets.

Internal attack | An attack in which an attacker is able to compromise a system's access controls and either establish a presence inside the network or place malware on an internal computer.

Internal-to-external attack | An attack in which the attacker uses an organization's infrastructure to launch an attack on another organization.

International Electrotechnical Commission (IEC) | An international, nonprofit organization that publishes global standards on electrotechnology, or all things electronic and electric.

International Information Systems Security Certification Consortium (ISC)² | A nonprofit professional and certification body that provides related programs for information security professionals.

International Organization for Standardization (ISO) | The world's largest publisher of worldwide standards.

International Professional Practices Framework (IPPF) | Mandatory practices and strongly recommended guidance published by the IIA.

International Telecommunication Union Telecommunication Standardization Sector (ITU-T) | One of three divisions of the International Telecommunication Union, primarily responsible for communications standards.

Internet Protocol (IP) address | A numerical representation that identifies a system node on a computer network.

Internet service provider (ISP) | An organization that provides a connection to the Internet.

Intrusion detection system (IDS) | A network hardware device or software that monitors real-time network activity and compares the observed behavior with performance thresholds and trends to detect unusual activity that might represent an intrusion.

Intrusion prevention system (IPS) | A network hardware device or software that monitors real-time network activity, compares the observed behavior with performance thresholds and trends to detect unusual activity that might represent an intrusion, and takes action to stop the attack.

Intrusive test | Any test that simulates an attack and results in damage.

ISACA | A global professional organization that provides resources and guidance relating to IT governance.

ISO/IEC 27001 | Good practices that provide an accepted baseline against which IT auditors can audit.

ISO/IEC 27002 | Good practices for information security management.

ISO/IEC 27005 | A security risk-management framework developed by ISO/IEC.

IT universe | All the resources or auditable components within an organization.

K

Kerberos | A popular computer network authentication protocol that allows nodes to prove their identities to one another.

L

LAN Domain | An IT domain composed of the equipment making up the local area network.

LAN-to-WAN Domain | An IT domain that bridges between the LAN and the WAN.

Least privilege | A principle that dictates that users have access only to what they need to perform their duties.

Local area network (LAN) | A computer network for communications between systems covering a small physical area.

Local resource | Any resource attached to a local computer—the same computer to which the user has logged on.

M

Malware | A term that refers to a collection of different types of software that share the goal of infiltrating a computer and making it do something.

Mandatory access control (MAC) | An access control method based on data classification and user clearance.

Media Access Control (MAC) address | A unique identifier assigned to most network adapters.

Metro Ethernet | Another name for an Ethernet MAN.

Multifactor authentication | A type of authentication that uses more than two methods to authenticate a user.

Multiprotocol Label Switching (MPLS) | A network mechanism that adds a simple label to each network packet, making routing of the packet faster than routing based on data in the header portion of the packet.

N

National Checklist Program (NCP) | A government repository of baseline security checklists.

National Institute of Standards and Technology (NIST) | An organization that promotes innovation and

competitiveness through the advancement of science, standards, and technology to improve economic security and quality of life.

Need to know | A subject has a need to access an object to complete a task.

Network Access Control (NAC) | A combination of security controls that define and implement a policy that describes the requirements to access your network.

Network monitoring platforms (NMPs) | A dedicated computer on the LAN running network management software.

Network operating system (NOS) | Software that provides the interface between the hardware and the Application Layer software.

Network scan | An automated method for discovering host systems on a network.

Networking devices | Hardware devices that connect other devices and computers using connection media.

Networking services software | Software that provides connection and communication services for users and devices.

NIST 800-30 | A guide developed by NIST for the management of risk for IT systems.

NIST 800-53 | Recommended security controls, developed by NIST.

NIST 800-53A | A guide for assessing security controls, developed by NIST.

NIST 800-115 | A technical guide published by NIST on conducting information security tests and assessments.

NIST Internal Reports (NISTIR) | NIST publications that describe niche technical research.

Node | Any computer or device that is connected to the network.

Non-disclosure agreement (NDA) | Another name for a confidentiality agreement.

Nonintrusive test | A test that only validates the existence of a vulnerability.

O

Object | The target of an access request, such as a file, folder, or other resource.

Objectives | A set of goals. Used as part of an assessment to determine what needs to be accomplished to validate a control.

Open Source Security Testing Methodology Manual (OSSTMM) | A peer-reviewed method that takes a scientific approach to security testing.

Open Systems Interconnection (OSI) reference model | A generic description for how computers use multiple layers of protocol rules to communicate across a network. The OSI reference model defines seven distinct layers.

Owner | A user who has complete control of an object, including the right to grant access to other users or groups.

P

Packet sniffer | Software that copies specified packets from a network interface to an output device, generally a file.

Paperwork Reduction Act of 1995 | A United States statute to further the goal of having federal agencies take more responsibility and be held more publicly accountable for reducing the paperwork they generate.

Payment Card Industry Data Security Council (PCI DSC) | The organization responsible for the development and maintenance of security standards for the payment card industry.

Payment Card Industry Data Security Standard (PCI DSS) | Industry-created standards to prevent payment card theft and fraud.

Penetration test | A method for assessing information systems in an attempt to bypass controls and gain access.

Permissions | The definitions of what object access actions are permitted for a specific user or group.

Plan-do-check-act (PDCA) | An iterative process for continuous improvement.

Policy | A document that regulates conduct through a general statement of beliefs, goals, and objectives.

Prescriptive control | Detailed and specific measures to be applied to a system.

Pretexting | The act of using false pretenses to obtain confidential information.

Preventive controls | Mechanisms that keep an undesired action from happening, such as locked doors or computer access controls.

Privacy management | The rights and obligations of individuals and organizations with regard to how they manage personal information.

Privacy officer | A senior-level management position within an organization responsible for handling privacy laws and their impact on the organization.

Procedure | A document that provides step-by-step instructions for how standards and guidelines are put into practice.

Process Capability Model | A maturity model that provides the framework to measure the performance of a given process. Based on the results, areas for improvement are identified.

Protected health information (PHI) | Individually identifiable health information.

Protocol | A set of rules that govern communication.

Proxy server | A type of firewall that makes requests for remote services on behalf of local clients.

Public Company Accounting Oversight Board (PCAOB) | An organization that provides oversight for public accounting firms and defines the process for compliance audits.

Q

Qualified Security Assessor (QSA) | Entities qualified and authorized to perform PCI compliance assessment.

R

RACI matrix | A table used to document tasks and the personnel responsible for the assignments. RACI stands for responsible, accountable, consulted, and informed.

Rack system | An open cabinet with tracks into which multiple computers can be mounted instead of mounting them in individual cases.

Red Flags Rule | A rule established by the Fair and Accurate Credit Transactions Act and implemented to prevent identity theft.

Regulatory agencies | Oversight agencies that deal with administrative law, codifying, and enforcing rules.

Remote Access Domain | An IT domain that covers the access infrastructure for users accessing remote systems.

Remote Authentication Dial In User Service (RADIUS) | A network protocol that supports remote connections by centralizing the management tasks for authentication, authorization, and accounting for computers to connect and access a network.

Remote resource Any resource accessible across the LAN.

Risk | An uncertainty that might lead to a loss. Losses occur when a threat exploits vulnerability.

Risk appetite | The degree of risk that an organization is willing to accept to achieve its goals.

Risk arrogance | Occurs when an organization does not adequately assess and plan for risks.

Risk assessment | An analysis of threats and vulnerabilities against assets. A risk assessment allows the risks to be prioritized.

Risk IT | A framework based on guiding principles to effectively manage risk. Developed by ISACA.

Risk management | The practice of identifying, assessing, controlling, and mitigating risks. Techniques to manage risk include avoiding, transferring, mitigating, and accepting the risk.

Risk Management Framework (RMF) | Activities defined by NIST to manage organizational risk.

Risk tolerance | The range of acceptance of risks to keep an organization within its appetite for risk.

Rootkit | Software that modifies or replaces one or more existing programs to hide the fact that a computer has been compromised.

Rotation of duties | The process of rotating employees into different functions or job roles.

Router | A network device that connects two or more separate networks.

S

SANS Institute | A popular source for information security knowledge, training, and certification. SANS is a for-profit institute owned by the Escal Institute of Advanced Technologies.

SANS Technology Institute | A SANS-related organization that provides graduate-level educational programs.

Sarbanes-Oxley Act | An act that was created in the wake of accounting scandals from the likes of Enron and WorldCom. This act set new accountability and corporate responsibility standards for public companies and accounting firms.

Scope creep | When the original plans or goals of a project expand. Common with projects, particularly poorly planned projects.

Secure Socket Tunneling Protocol (SSTP) | A VPN protocol developed by Microsoft to provide a solution that works on any networking hardware. SSTP uses Secure Sockets Layer (SSL) to transport Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol (L2TP) traffic.

Secure VPNs | VPNs in which all traffic is encrypted.

Security configuration management (SCM) | The processes and techniques for managing security-related configuration items that directly relate to controls or settings.

Separation of duties | The process of dividing roles and responsibilities so a single individual can't undermine a critical process.

Server Message Block (SMB) | An Application Layer protocol commonly used to provide access to file shares and printers.

Service | A set of software functionality that a client accesses using a prescribed interface.

Service level agreement (SLA) | A portion of a service contract that promises specific levels of service.

Service Organization Control (SOC) reports | Auditing standards maintained by the AICPA.

Simple Network Management Protocol (SNMP) | A network protocol used to monitor network devices.

Single point of failure | Any component on which service relies. If the single component fails, all other dependent components essentially fail as well.

Social engineering | The act of manipulating people into divulging information.

Software configuration management (SCM) | A formal method for managing changes to a software application.

Source code | Text files of programs that developers compile into application programs that computers can run.

Special Publications | A series of standards developed by NIST.

Spyware | Software that covertly collects information without the user's knowledge or permission.

Standard | A document that supports a policy. It consists of mandated rules, which support the higher-level policy goals.

Statement on Standards for Attestation

Engagements No. 16 (SSAE 16) | A report that is intended to provide assurance to organizations (user entities). This report replaces the SAS 70 report.

Storage area network (SAN) | A collection of storage devices that is attached to a network in such a way that the devices appear to be local storage devices.

Subject | A user or object that requests to access a file, folder, or other resource.

Subnet | A subsection, or part, of a network.

Switch | A networking device that forwards input it receives only to the appropriate output port.

System Security Certified Practitioner (SSCP) | An (ISC)² certification that tests candidates for knowledge of security concepts appropriate for IT security practitioners.

System/Application Domain | An IT domain that covers network systems, applications, and software for users.

T

Terminal Access Controller Access-Control System Plus (TACACS+) | A network protocol developed by Cisco. TACACS+ provides access control for remote networked computing devices using one or more centralized servers.

Threat | Any activity that represents a possible danger.

Threat actions | The methods of carrying out a particular threat.

Threat identification | The process of identifying all threats to the organization.

Time to recover (TTR) | The acceptable amount of time that is allowed to repair or replace failed components. Also called time to repair.

The TJX Companies, Incorporated | A large off-price retailer of apparel and home fashions that suffered one of the most severe breaches of private data in history.

Tokenization | An alternative to encryption. Rather than encrypting data, tokenization simply substitutes a randomly generated value for the data.

Traffic-monitoring devices | Devices that monitor network traffic and compare performance with a baseline.

Transmission Control Protocol/Internet Protocol (TCP/IP) | The basic protocol, or language, of modern networks and the Internet.

Transmission Control Protocol/Internet Protocol (TCP/IP) reference model | A generic description for how computers use multiple layers of protocol rules to communicate across a network. The TCP/IP reference model defines four different layers of communication rules.

Transparent Data Encryption (TDE) | A method of encrypting an entire database that is transparent to the user and requires no input or action.

Trojan horse | Software that either hides or masquerades as a useful or benign program.

Tunneling | A technique that creates a virtual encrypted connection and allows applications to use any protocol to communicate with servers and services without having to worry about addressing or privacy concerns.

Two-factor authentication | A type of authentication that uses two types of authentication to authenticate a user.

Type I authentication (what you know) | The information that only a valid user knows. The most common examples of Type I authentication are a password or PIN.

Type II authentication (what you have) | A physical object that contains identity information, such as a token, card, or other device.

Type III authentication (what you are) | A physical characteristic (biometric), such as a fingerprint, handprint, or retina characteristic.

U

Uninterruptible power supply (UPS) | A device that provides continuous usable power to one or more

devices.

User Datagram Protocol (UDP) | A core protocol of the Internet Protocol suite. UDP is a connectionless protocol, which provides no guarantee of delivery.

User Domain | An IT domain that covers the end users of information systems.

V

Val IT | A framework that governs IT investments, created by ISACA.

Virtual machines | Software programs that look and run like a physical computer.

Virtual private network (VPN) | A persistent connection between two nodes that allows bidirectional communication as if the connection were a direct connection with both nodes in the same network.

Virus | A software program that attaches itself to or copies itself into another program for the purpose of causing the computer to follow instructions that were not intended by the original program developer.

Vulnerability | A weakness.

Vulnerability analysis | The examination of weaknesses or flaws.

Vulnerability scan | An automated method for testing a system's services and applications for known security holes.

W

WAN Domain | An IT domain that covers the equipment and activities outside the LAN and beyond the LAN-to-WAN Domain.

WAN optimizers | Network devices or software that can analyze current WAN performance and then modify how new traffic is sent across the WAN.

WAN service provider | An organization that provides access to its wide area network for a fee.

Wardialing | The process of instructing a computer to dial many telephone numbers looking for modems on the other end.

Wardriving | Using a laptop or other mobile device to quickly find wireless networks while driving around in a motor vehicle.

Wide area network (WAN) | A network covering a large area often connecting multiple LANs.

Wireless local area network (WLAN) | A wireless network covering a small physical area, such as an office or building.

Workstation Domain | The operating environment of an end user.

WorldCom | A large U.S.-based telecommunications company involved in a massive accounting scandal, which ultimately forced it to file bankruptcy in 2002.

Worm | A self-contained program that replicates and sends copies of itself to other computers, generally across a network.

References

- 15 U.S. Code Chapter 94, Subchapter I—Disclosure of Nonpublic Personal Information, n.d. Legal Information Institute. <https://www.law.cornell.edu/uscode/text/15/chapter-94/subchapter-I> (accessed May 4, 2015).
- American Institute of Certified Public Accountants. Generally Accepted Privacy Principles. n.d. American Institute of Certified Public Accountants. <http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GEN> (accessed April 19, 2015).
- _____. New SOC Reports for Service Organizations Replace SAS 70 Reports, 2011. American Institute of Certified Public Accountants. http://www.cpa2biz.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2011/CPA/Fel (accessed April 19, 2015).
- _____. SOC Reports Information for CPAs, n.d. American Institute of Certified Public Accountants. <http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/CPAs.aspx> (accessed April 19, 2015).
- Beresford, Dennis R., Nicholas deB. Katzenbach, and C. B. Rogers, Jr. Report of Investigation by the Special Investigative Committee of the Board of Directors of WorldCom, Inc., March 13, 2003. U.S. Securities and Exchange Commission. <http://www.sec.gov/Archives/edgar/data/723527/000093176303001862/dex991.htm> (accessed April 19, 2015).
- Cannings, Rich, Himanshu Dwivedi, and Zane Lackey. *Hacking Exposed Web 2.0: Web 2.0 Security Secrets and Solutions*. New York: McGraw-Hill Professional, 2008.
- Cannon, David L., Timothy S. Bergmann, and Brady Pamplin. *CISA: Certified Information Systems Auditor Study Guide*. Indianapolis: Sybex, Wiley Publishing, 2006.
- Celender, Jennifer. Information Privacy Topics, A Discussion, 2002. SANS Institute. http://www.sans.org/reading_room/whitepapers/privacy/information_privacy_topics_a_discussion_6 (accessed April 19, 2015).
- Children's Internet Protection Act, 2001. Internet Free Expression Alliance. ifea.net/cipa.pdf (accessed April 19, 2015).
- Clarke, Steve. *End-user Computing: Concepts, Methodologies, Tools, and Applications*. Hershey, PA: IGI Publishing, 2008.
- Committee of Sponsoring Organizations of the Treadway Commission. About Us, 2010. Committee of Sponsoring Organizations of the Treadway Commission. <http://www.coso.org/aboutus.htm> (accessed April 19, 2015).
- _____. Guidance, 2010. Committee of Sponsoring Organizations of the Treadway Commission. <http://www.coso.org/guidance.htm> (accessed April 19, 2015).
- Contesti, Diana-Lynn, Douglas Andre, Eric Waxvik, Paul A. Henry, and Bonnie A. Goins. *Official (ISC)² Guide to the SSCP CBK*. Boca Raton, FL: Auerbach Publications, Taylor & Francis Group, 2007.
- Davis, Chris, Mike Schiller, and Kevin Wheeler. *IT Auditing: Using Controls to Protect Information Assets*. 1st ed. New York: The McGraw-Hill Companies, 2007.
- Ethics Working Group. Ethics Working Group, n.d. Ethics Working Group. <http://ethics-wg.org/> (accessed April 19, 2015).
- Fair and Accurate Credit Transactions Act of 2003. 2003. U.S. Government Publishing Office. <http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf> (accessed April 19, 2015).
- Family Educational Rights and Privacy Act (FERPA). n.d. U.S. Department of Education. <http://www2.ed.gov/policy/gen/guid/fpcos/ferpa/index.html> (accessed April 19, 2015).
- Federal Deposit Insurance Corporation. Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information), n.d. Federal Deposit Insurance Corporation. <https://www.fdic.gov/regulations/compliance/manual/pdf/VIII-1.1.pdf> (accessed April 19, 2015).
- Gallegos, Frederick, and Sandra Senft. *Information Technology Control and Audit*, 3rd ed. Boca Raton, FL:

- Auerbach Publications, Taylor & Francis Group, 2008.
- Global Information Assurance Certification. Certifications, n.d. Global Information Assurance Certification. <http://www.giac.org/certifications> (accessed May 4, 2015).
- Hamid, Rafidah Abdul. Wireless LAN: Security Issues and Solutions, 2003. SANS Institute. http://www.sans.org/reading_room/whitepapers/wireless/wireless-lan-security-issuesolutions_1009 (accessed April 19, 2015).
- Herzog, Pete. Open Source Security Testing Methodology Manual (OSSTMM). n.d. Institute for Security and Open Methodologies. <http://www.isecom.org/osstmm/> (accessed April 19, 2015).
- Heschl, Jimmy. COBIT in Relation to Other International Standards, 2004. ISACA. <http://www.isaca.org/Journal/archives/2004/Volume-4/Documents/jpdf044-COBITinRelationtoOther.pdf> (accessed April 19, 2015).
- H. R. 2458, n.d. National Institute of Standards and Technology. <http://csrc.nist.gov/drivers/documents/HR2458-final.pdf> (accessed April 19, 2015).
- H. R. 2458–48. National Institute of Standards and Technology. <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf> (accessed April 19, 2015).
- IEEE Standards Association. IEEE Get Program, n.d. IEEE Standards Association. <http://standards.ieee.org/about/get/802/802.11.html> (accessed April 19, 2015).
- Information Assurance Support Environment. Policy and Guidance Home, n.d. Information Assurance Support Environment. <http://iase.disa.mil/Pages/index.aspx> (accessed May 4, 2015).
- The Institute of Internal Auditors. Code of Ethics—English, The Institute of Internal Auditors. 2010. <http://www.theiia.org/guidance/standards-and-guidance/ippf/code-of-ethics/> (accessed April 19, 2015).
- . The Institute of Internal Auditors, n.d. The Institute of Internal Auditors. <https://na.theiia.org/standards-guidance/topics/Pages/Information-Technology.aspx> (accessed May 4, 2015).
- . Reference Library: Audit Software, n.d. The Institute of Internal Auditors. <http://www.theiia.org/itauditarchive/index.cfm?act=ITAudit.reflibcategory&catid=7> (accessed April 19, 2015).
- . Welcome to the IIA, 2010. The Institute of Internal Auditors. <http://www.theiia.org/> (accessed April 19, 2015).
- International Federation of Accountants. Defining and Developing an Effective Code of Conduct for Organizations, 2007. International Federation of Accountants. <http://www.ifac.org/publications-resources/defining-and-developing-effective-code-conduct-organizations> (accessed May 4, 2015).
- International Organization for Standardization. ISO/IEC 27002:2013(en), n.d. International Organization for Standardization. <https://www.iso.org/obp/ui/#iso:std:54533:en> (accessed April 19, 2015).
- . ISO/IEC 27001:2013—Information Technology—Security Techniques—Information Security Management Systems—Requirements, 2013. International Organization for Standardization. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534 (accessed April 19, 2015).
- International Telecommunication Union. X.701 Information Technology—Open Systems Interconnection—Systems Management Overview, 1997. International Telecommunication Union. <http://www.itu.int/rec/T-REC-X.701-199708-I> (accessed April 19, 2015).
- ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, 2012. ISACA. <http://www.isaca.org/COBIT/Documents/COBIT5-Ver2-FrameWork.pdf> (accessed April 19, 2015).
- . COBIT 5 Introduction, 2012. ISACA. <http://www.isaca.org/COBIT/Documents/COBIT5-Introduction.ppt> (accessed April 19, 2015).
- . COBIT 5 Resource Center, n.d. ISACA. <https://cobitonline.isaca.org> (accessed April 19, 2015).
- . Code of Professional Ethics, n.d. ISACA. <http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx> (accessed May 4, 2015).
- . Identify, Govern, and Manage IT Risk Part 1: Risk IT Based on COBIT Objectives and Principles, 2009. ISACA. <http://www.isaca.org/Journal/archives/2009/Volume-4/Documents/jpdf094-identify-govern.pdf> (accessed May 4, 2015).

- _____. IS Auditing Procedure Security Assessment—Penetration Testing and Vulnerability Analysis. 2004. University of North Carolina Wilmington. <http://www.csb.uncw.edu/people/IvancevichD/classes/MSA%20516/Extra%20Readings%20on%20/> (accessed May 4, 2015).
- _____. IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals, 2010. ISACA. <http://www.isaca.org/knowledge-center/standards/documents/it-audit-assurance-guidance-1march2010.pdf> (accessed May 4, 2015).
- _____. Standards for IT Audit and Assurance, n.d. ISACA. <http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/Standards-for-IT-Audit-and-Assurance-English.aspx> (accessed April 19, 2015).
- _____. The COBIT 5 Process Capability Model. In *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL: ISACA, 2012.
- (ISC)². (ISC)² Code of Ethics, 2010. (ISC)². <http://www.isc2.org/ethics/default.aspx> (accessed April 19, 2015).
- ISOTC. ISO/IEC JTC 001 “Information Technology,” 2010. International Organization for Standardization. <http://isotc.iso.org/livelink/livelink/open/jtc1> (accessed April 19, 2015).
- IT Governance Institute. About the IT Governance Institute. n.d. IT Governance Institute. <http://www.itgi.org/> (accessed April 19, 2015).
- _____. Unlocking Value: An Executive Primer on the Critical Role of IT Governance. n.d. IT Governance Institute. http://www.isaca.org/knowledge-center/research/documents/unlocking-value-an-executive-primer-on-the-critical-role-of-it-governance_res_eng_1108.pdf (accessed May 4, 2015).
- Kidder, Rushworth. *How Good People Make Tough Choices Resolving the Dilemmas of Ethical Living*. Clovis, CA: Quill, 2003.
- King, Tom. Packet Sniffing in a Switched Environment, 2006. SANS Institute. http://www.sans.org/reading_room/whitepapers/networkdevs/packet-sniffing-switched-environment_244 (accessed April 19, 2015).
- KPMG. KPMG’s Code of Conduct—Our Promise of Professionalism, n.d. KPMG. <http://www.kpmg.com/us/en/about/pages/codeofconduct.aspx> (accessed May 4, 2015).
- Kurihara, Yutaka, et al. *Information Technology and Economic Development*. Hershey, PA: IGI Publishing, 2008.
- LAN Switch Security: What the Hackers Know That You Don’t. *Network World* 24, no. 45 (2007):8.
- Leo, Ross. *The HIPAA Program Reference Handbook*. Boca Raton, FL: CRC Press, 2005.
- Littman, Marlyn Kemper. *Building Broadband Networks*. Boca Raton, FL: CRC Press, 2002.
- National Institute of Standards and Technology. Computer Security Resource Center, n.d. National Institute of Standards and Technology. <http://csrc.nist.gov/> (accessed April 19, 2015).
- _____. Federal Information Security Management Act (FISMA) Implementation Project, n.d. National Institute of Standards and Technology. <http://csrc.nist.gov/groups/SMA/fisma/index.html> (accessed April 19, 2015).
- _____. Guide for Assessing the Security Controls in Federal Information Systems and Organizations, 2010. National Institute of Standards and Technology. <http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf> (accessed April 19, 2015).
- _____. Guide for Conducting Risk Assessments, 2012. National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (accessed May 4, 2015).
- _____. Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework, n.d. National Institute of Standards and Technology. <http://nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf> (accessed April 19, 2015).
- _____. Information Security Handbook: A Guide for Managers, 2006. National Institute of Standards and Technology. <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100 -Mar07-2007.pdf> (accessed April 19, 2015).
- _____. The NIST Definition of Cloud Computing, 2011. National Institute of Standards and Technology. <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> (accessed April 19, 2015).
- _____. Security and Privacy Controls for Federal Information Systems and Organizations, 2013. National Institute of Standards and Technology.

- <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> (accessed April 19, 2015).
- _____. Special Publications (800 Series), n.d. National Institute of Standards and Technology. <http://csrc.nist.gov/publications/PubsSPs.html> (accessed April 19, 2015).
- _____. Technical Guide to Information Security Testing and Assessment, 2008. National Institute of Standards and Technology. <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf> (accessed April 19, 2015).
- Oud, Ernst. The Value to IT of Using International Standards, 2005. ISACA. <http://www.isaca.org/Journal/archives/2005/Volume-3/Documents/jpdf053-The-Value-to-IT-Using.pdf> (accessed May 4, 2015).
- Paperwork Reduction Act of 1995. n.d. U.S. Small Business Administration. <https://www.sba.gov/sites/default/files/files/pap.pdf> (accessed April 19, 2015).
- PCI Security Standards Council. PCI SSC Data Security Standards Overview, n.d. PCI Security Standards Council. https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (accessed April 19, 2015).
- _____. Welcome to the PCI Security Standards Council, n.d. PCI Security Standards Council. <https://www.pcisecuritystandards.org> (accessed April 19, 2015).
- Powers, Jr., William C., Raymond S. Troubh, and Herbert S. Winokur, Jr. Report of Investigation by the Special Investigative Committee of the Board of Directors of Enron Corp. FindLaw. <news.findlaw.com/wp/docs/enron/specinv020102rpt1.pdf> (accessed April 19, 2015).
- Public Company Accounting Oversight Board. Auditing, n.d. Public Company Accounting Oversight Board. <http://pcaobus.org/Standards/Auditing/Pages/default.aspx> (accessed April 19, 2015).
- _____. Auditing Standard No. 2, n.d. Public Company Accounting Oversight Board. http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_2_Appendix_E.aspx (accessed April 19, 2015).
- _____. Auditing Standard No. 3, n.d. Public Company Accounting Oversight Board. http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_3.aspx (accessed April 19, 2015).
- _____. Auditing Standard No. 5, 2010. Public Company Accounting Oversight Board. http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx (accessed April 19, 2015).
- _____. PCAOB Oversees the Auditors of Companies to Protect Investors, n.d. Public Company Accounting Oversight Board. <http://pcaobus.org/Pages/default.aspx> (accessed April 19, 2015).
- RFC 1087—Ethics and the Internet, 1989. Internet Engineering Task Force Tools. <http://tools.ietf.org/html/rfc1087> (accessed April 19, 2015).
- SANS Institute. Critical Security Control: 2.0, n.d. SANS Institute. <https://www.sans.org/critical-security-controls/control/20> (accessed May 4, 2015).
- _____. The Most Trusted Source for Computer Security Training, Certification, and Research, n.d. SANS Institute. <http://www.sans.org/> (accessed April 19, 2015).
- SANS Technology Institute. SANS Technology Institute, n.d. SANS Technology Institute. <http://www.sans.edu/> (accessed April 19, 2015).
- Sarbanes-Oxley Act of 2002, n.d. SEC. <https://www.sec.gov/about/laws/soa2002.pdf> (accessed April 19, 2015).
- Sayana, S. Anantha. Using CAATs to Support IS Audit, 1, 2003. ISACA. <http://www.isaca.org/Journal/archives/2003/Volume-1/Documents/jpdf031-UsingCAATstoSupportISAu.pdf> (accessed May 4, 2015).
- Schneier, Bruce. The Psychology of Security (Part 1), 2008. Schneier on Security. <http://www.schneier.com/essay-155.html> (accessed April 19, 2015).
- Subramanian, Ramesh. *Computer Security, Privacy, and Politics: Current Issues, Challenges and Solutions*. Hershey, PA: IGI Publishing, 2008.
- Talukder, Asoke K., and Manish Chaitanya. *Architecting Secure Software Systems*. Boca Raton, FL: CRC Press, 2008.
- Tipton, Harold, and Micki Krause. *Information Security Management Handbook*. 6th ed. Boca Raton, FL: Auerbach Publications, Taylor & Francis Group, 2007.
- _____. *Information Security Management Handbook*, 6th ed., vol. 3. Chicago: Auerbach Publications, 2009.

- Tyson, Jeff. How LAN Switches Work, 2010. HowStuffWorks. <http://www.howstuffworks.com/lan-switch.htm> (accessed April 19, 2015).
- U.S. Department of Health & Human Services. HIPAA Administrative Simplification Statute and Rules, n.d. U.S. Department of Health & Human Services.
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html> (accessed April 19, 2015).
- _____. HIPAA Administrative Simplification, 2013. U.S. Department of Health & Human Services.
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification -201303.pdf> (accessed April 19, 2015).
- _____. Standards for Privacy of Individually Identifiable Health Information, 2002. U.S. Department of Health & Human Services.
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/privrule/privruletxt.txt> (accessed April 19, 2015).
- _____. Understanding Health Information Privacy, n.d. U.S. Department of Health & Human Services.
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html> (accessed April 19, 2015).
- U.S. Federal Communications Commission. Children's Internet Protection Act (CIPA). 2015. U.S. Federal Communications Commission. <http://transition.fcc.gov/cgb/consumerfacts/cipa.pdf> (accessed April 19, 2015).
- _____. Children's Internet Protection Act. n.d. U.S. Federal Communications Commission. n.d.
<http://www.fcc.gov/guides/childrens-internet-protection-act> (accessed April 19, 2015).
- U.S. Federal Trade Commission. Fighting Fraud with the Red Flags Rule: A How-To Guide for Business, n.d. Federal Trade Commission. <http://ftc.gov/redflagsrule> (accessed April 19, 2015).
- U.S. Government Accountability Office. Financial Audit Manual (FAM), 2008. U.S. Government Accountability Office. <http://www.gao.gov/special.pubs/gaopcie/> (accessed April 19, 2015).
- U.S. Government Publishing Office. Electronic Code of Federal Regulations, 2015. U.S. Government Publishing Office. <http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=11975031b82001bed902b3e73f33e604&rgn=div5&view=text&node=34:1.1.1.1.33&idno=34> (accessed April 19, 2015).
- U.S. Securities and Exchange Commission. The Laws That Govern the Securities Industry, n.d. U.S. Securities and Exchange Commission. <http://www.sec.gov/about/laws.shtml> (accessed April 19, 2015).
- Wakefield, Robin L. Employee Monitoring and Surveillance—The Growing Trend, 2004. ISACA.
<http://www.isaca.org/Journal/archives/2004/Volume-1/Documents/jpdf041 - EmployeeMonitoringand.pdf> (accessed May 4, 2015).
- Wright, Craig S. *The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments*. Burlington, MA: Syngress, 2008.

Index

The index that appeared in the print version of this title was intentionally removed from the eBook. Please use the search function on your eReading device to search for terms of interest. For your reference, the terms that appear in the print index are listed below.

- 10 U.S. Code Section 2223, Information Technology: Additional Responsibilities of Chief Information Officers
- 10 U.S. Code Section 2224, Defense Information Assurance Program

A

- acceptable use policy (AUP)
- access control lists (ACLs)
- access controls
- access rights
- accountabilities
- accounting management
- accreditation
- ACLs. *See* access control lists
- activity objects
- acts of congress
- administration
- administration management
- administrative safeguards, HIPAA
- Administrative Simplification
- AICPA. *See* American Institute of Certified Public Accountants
- alternative controls
- American Institute of Certified Public Accountants (AICPA)
- American National Standards Institute (ANSI)
- American Recover and Reinvestment Act (ARPA)
- analog modem
- analytical skills
- annex A
- annual employee performance review
- annual security compliance audit
- anonymous users
- ANSI. *See* American National Standards Institute
- antivirus software
- application connection encryption
- application controls
- application data encryption
- application encryption
- Application Layer firewall
- application performance monitoring software
- application server
- application software
- application software patch management
- applications
- “Applying a Single Integrated Framework”
- Approved Scanning Vendor (ASV)
- ARPA. *See* American Recover and Reinvestment Act
- Arthur Andersen firm

assessments
asset management
assurance
ASV. *See* Approved Scanning Vendor
attack execution
attack planning
attacks
audit department Web site
audit finding
audit frequency
audit logs
audit objective
audit scope
audit validating compliance process
auditing
Auditing Standard No. 2
Auditing Standard No. 5
Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA)
auditors
audits
AUP. *See* acceptable use policy
authentication
authentication servers
authorization
automated audit reporting tools and methodologies
automated/computer-based tool
automated vulnerability assessment tool
availability
awareness

B

background check
backup encryption
backup image
backups
baseband techniques
baseline
baseline configuration management
baseline controls
BCPs. *See* business continuity plans
behavioral skills
best practice documents
black-box testing
blacklist
BMIS. *See* Business Model for Information Security
breadth
broadband
business continuity
business continuity management
business continuity plans (BCPs)
business drivers
business logic
Business Model for Information Security (BMIS)
business writing skills

C-I-A triad. *See* confidentiality, integrity, and availability triad
C&A. *See* certification and accreditation
CAATT. *See* computer assisted audit tools and techniques
CAG. *See* Consensus Audit Guidelines
Canadian Institute of Chartered Accountants (CICA)
cancer
CAP. *See* Certification and Accreditation Professional
card verification value (CVV) number
career opportunities for IT auditing
CASP. *See* CompTIA Advanced Security Practitioner
CBK. *See* Common Body of Knowledge
CCB. *See* configuration control board
CCFP. *See* Certified Cyber Forensics Professional
CCSA. *See* Certification in Control Self-Assessment
cell relay WAN
certification and accreditation (C&A)
Certification and Accreditation Professional (CAP)
Certification for IT auditing
Certification in Control Self-Assessment (CCSA)
Certification in Risk Management Assurance (CRMA)
Certified Cyber Forensics Professional (CCFP)
Certified Financial Services Auditor (CFSAs)
Certified Government Auditing Professional (CGAP)
Certified in Risk and Information Systems and Control (CRISC)
Certified in the Governance of Enterprise IT (CGEIT)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
Certified Information Systems Security Professional (CISSP)
Certified Internal Auditor (CIA) certification
Certified Public Accountants (CPAs)
Certified Secure Software Lifecycle Professional (CSSLP)
CEUs. *See* continuing education units
CFSAs. *See* Certified Financial Services Auditor
CGAP. *See* Certified Government Auditing Professional
CGEIT. *See* Certified in the Governance of Enterprise IT
change management
changing technology
chief information officer (CIO)
chief information security officers (CISOs)
chief privacy officer (CPO)
Child Online Protection Act
Children's Internet Protection Act (CIPA)
Children's Online Privacy Protection Act (COPPA)
CIA certification. *See* Certified Internal Auditor certification
CICA. *See* Canadian Institute of Chartered Accountants
CIO. *See* chief information officer
CIPA. *See* Children's Internet Protection Act
ciphertext
circuit switching WAN
circumstance
CISA. *See* Certified Information Systems Auditor
Cisco VPN Monitor
CISM. *See* Certified Information Security Manager
CISOs. *See* chief information security officers

CISSP. *See* Certified Information Systems Security Professional
cleartext
client based architecture
client/server architecture
client/server protocol
Clinger-Cohen Act of 1996
cloud computing
CMDB. *See* configuration management database
CMOS configuration. *See* complementary metal-oxide semiconductor configuration
coaxial cable
COBIT. *See* Control Objectives for Information and Related Technology
COBIT 5
code of conduct
code of ethics
CodePlex Remote Access Monitor
cold site
Committee of Sponsoring Organizations (COSO)
Committee of Sponsoring Organizations (COSO) of the Treadway Commission
Common Body of Knowledge (CBK)
Common Vulnerabilities and Exposures (CVE)
communication
communication protocol
communication skills
Communications Decency Act
communications security
compensating controls
competency
complementary metal-oxide semiconductor (CMOS) configuration
complexity
compliance
compliance auditing
components
comprehensive security assessments
CompTIA. *See* Computing Technology Industry Association
CompTIA Advanced Security Practitioner (CASP)
CompTIA Project+certification
CompTIA Security + certification
computer assisted audit tools and techniques (CAATT)
computer performance
computer room
Computer Security Division (CSD) of NIST
Computing Technology Industry Association (CompTIA)
confidentiality
confidentiality agreement
confidentiality, integrity, and availability (C-I-A) triad
configuration
configuration and change management
configuration change control board
configuration control board (CCB)
configuration management
configuration management database (CMDB)
configuration monitoring and auditing
configuration validation
connection media
Consensus Audit Guidelines (CAG)
content analysis

content keyword filtering
continuing education units (CEUs)
continuous monitoring
continuous power
contractors
control activities
control analysis process
control classification
control objectives
Control Objectives for Information and Related Technology (COBIT)
control recommendations process
control self-assessments (CSAs)
control standards
controls
cooperative agreement
coordinated attacks
COPPA. *See* Children's Online Privacy Protection Act
Corporate Accountability and Responsibility Act
Corporate Fraud Accountability Act of 2002
corrective controls
COSO. *See* Committee of Sponsoring Organizations
cost
countermeasure gap analysis
countermeasures
coverage
“Covering the Enterprise End to End”
CPAs. *See* Certified Public Accountants
CPO. *See* chief privacy officer
credit card breach
credit card industry
creditor
CRISC. *See* Certified in Risk and Information Systems and Control
criteria
Critical Security Controls
Critical Security Controls for Effective Cyber Defense
CRMA. *See* Certification in Risk Management Assurance
cryptographic controls
cryptography
CSAs. *See* control self-assessments
CSD of NIST. *See* Computer Security Division of NIST
CSSLP. *See* Certified Secure Software Lifecycle Professional
CVE. *See* Common Vulnerabilities and Exposures
CVV number. *See* card verification value number
cybersecurity
Cybersecurity Framework

D

DAC. *See* discretionary access control
data access
data centers
data isolation
data leak security appliances
data loss security appliances
data privacy
data privacy protection

data-protection methods
data storage
data storage devices
database and drive encryption
database encryption
database servers host data
databases
Datagram Transport Layer Security (DTLS)
dedicated line/leased line WAN
dedicated lines
demilitarized zone (DMZ)
Deming cycle
denial of service (DoS) attack
depth
descriptive control framework
desktop computers
detective controls
devices
dial-in penetration testing
dial-up connections
diesel generators
digital certificates
directory information
disaster recovery
disaster recovery plans (DRPs)
discretionary access control (DAC)
distributed applications
distributed architectures
DMZ. *See* demilitarized zone
DNS. *See* Domain Name System
document review
documentation
documented IT security policies
DoD requirements. *See* U.S. Department of Defense requirements
Domain Name System (DNS)
Domains in the IT infrastructure
DoS attack. *See* denial of service attack
DRPs. *See* disaster recovery plans
DTLS. *See* Datagram Transport Layer Security
dual-homed ISP connections
dual routers/dual circuits
due care
due diligence

E

E-Government Act of 2002
E-mail AUPs
e-mail policy
E-Rate discounts
education for IT auditor
effective risk-assessment process
Electronic Communications Privacy Act of 2000
electronic PHI (ePHI)
electronic work papers
employee background checks

employee handbook
employees
employer-driven codes of conduct
employment policies
enabler goals
“Enabling a Holistic Approach”
encapsulating protocol
encryption
Enforcement Rule
Enron Corporation
enterprise risk management (ERM)
enumeration
environment control
Environmental Protection Agency (EPA)
environmental security
EPA. *See* Environmental Protection Agency
ePHI. *See* electronic PHI
ERM. *See* enterprise risk management
Ethernet
Ethernet MAN
ethical behavior principles
ethics
Ethics Working Group
event correlation
event identification, COSO framework
examination method
executive summary
external auditors
external compliance
external media
external to internal penetration test

F

Fair and Accurate Credit Transactions Act of 2003
Fair Credit Reporting Act (FCRA)
Family Educational Rights and Privacy Act (FERPA)
fault management
FCAPS
FCC. *See* Federal Communications Commission
FCRA. *See* Fair Credit Reporting Act
FDA. *See* Food and Drug Administration
feasibility
Federal Communications Commission (FCC)
Federal Information Processing Standards (FIPS)
Federal Information Security Management Act of 2002 (FISMA)
Federal Trade Commission (FTC)
FERPA. *See* Family Educational Rights and Privacy Act
fiber optic cable
file encryption
file integrity checking
file server
file system
financial audits
financial institution
Financial Modernization Act of 1999

Financial Privacy Rule
finding
fingerprinting
FIPS. *See* Federal Information Processing Standards fire-suppression equipment
firewalls
FISMA. *See* Federal Information Security Management Act of 2002
fixed hard disk drives
flowcharting software
folder/directory encryption
Food and Drug Administration (FDA)
footprinting
frameworks
FTC. *See* Federal Trade Commission
FUD (fear, uncertainty, and doubt)

G

G2700. *See* GIAC Certified ISO-2700 Specialist
GAIT. *See* Guide to the Assessment of IT Risk
gap analysis
Generally Accepted Privacy Principles (GAPP)
generators
Generic Routing Encapsulation (GRE)
GIAC. *See* Global Information Assurance Certification
GIAC Certified ISO-2700 Specialist (G2700)
GIAC Expert Level certification program
GIAC Gold program
GIAC Systems and Network Auditor (GSNA) certification
Glass-Steagall Act
GLBA. *See* Gramm-Leach-Bliley Act
Global Information Assurance Certification (GIAC)
Global Technology Audit Guides (GTAGs)
governance
governance enablers
governance scope
Gramm-Leach-Bliley Act (GLBA)
gray-box testing
GRE. *See* Generic Routing Encapsulation
Group Policy Management Editor
GSNA certification. *See* GIAC Systems and Network Auditor certification
GTAGs. *See* Global Technology Audit Guides
guests/third parties
Guide to the Assessment of IT Risk (GAIT)
Guide to the Project Management Body of Knowledge, A (PMBOK)
guidelines

H

halon
hard disk drives
HCISPP. *See* Healthcare Information Security and Privacy Practitioner
Health Information Technology for Economic and Clinical Health (HITECH) Act
Health Insurance Portability and Accountability Act (HIPAA)
Healthcare Information Security and Privacy Practitioner (HCISPP)

Heartland Payment Systems
heating, ventilating, and air conditioning (HVAC) services
HHS. *See* U.S. Department of Health and Human Services
high-impact system baseline control
high-impact systems
high-level security assessment
high-speed internal LAN
HIPAA. *See* Health Insurance Portability and Accountability Act
HITECH Act. *See* Health Information Technology for Economic and Clinical Health Act
home alarm system
honeypot
host based architecture
hot site
HR. *See* human resources
HTTP. *See* Hypertext Transfer Protocol
HTTPS. *See* Hypertext Transfer Protocol Secure
hub
human resource security
human resources (HR)
HVAC services. *See* heating, ventilating, and air conditioning services
hybrid auditing framework or approach
Hypertext Transfer Protocol (HTTP)
Hypertext Transfer Protocol Secure (HTTPS)

I

IA. *See* information assurance
identification
identity theft
IDS. *See* intrusion detection system
IEC. *See* International Electrotechnical Commission
IEEE. *See* Institute of Electrical and Electronics Engineers
IEEE 802.11
IFAC. *See* International Federation of Accountants
IIA. *See* Institute of Internal Auditors
immediate response
impact
impact analysis process
in the clear
information assets, protection of
information assurance (IA)
information resource management (IRM)
information security (IS)
information security incident management
information security management system (ISMS)
information security policies
information security responsibilities
Information Systems Audit and Control Association (ISACA)
Information Systems Security Accountability
Information Systems Security Assessment Framework (ISSAF)
Information Systems Security Association (ISSA)
information systems types
information technology (IT)
Information Technology Assurance Framework (ITAF)
information technology audits
Information Technology Governance Institute (ITGI)

Information Technology Laboratory (ITL) Bulletins
infrastructure controls
Institute of Electrical and Electronics Engineers (IEEE)
Institute of Internal Auditors (IIA)
integrated audits
integrity
intellectual property rights (IPRs)
internal attack
Internal Auditor magazine
internal auditors
internal compliance
internal environment, COSO framework
internal penetration testing
internal standards
internal-to-external attack
internal to external penetration test
International Electrotechnical Commission (IEC)
International Federation of Accountants (IFAC)
International Information Systems Security Certification Consortium (ISC)²
International Organization for Standardization (ISO)
International Organization for Standardization/International Electrotechnical Commission (ISO/IEC)
 27002 standard
International Professional Practices Framework (IPPF)
International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
Internet AUPs
internet-facing components
Internet penetration testing
Internet Protocol (IP) addresses
Internet Protocol Security (IPSec)
Internet Protocol Suite
Internet service providers (ISPs)
Internet users
interview method
interviewing skills
interviews
intrusion detection system (IDS)
intrusion prevention system (IPS)
intrusive testing
investigative audits
IP addresses. *See* Internet Protocol addresses
IPPF. *See* International Professional Practices Framework
IPS. *See* intrusion prevention system
IPSec. *See* Internet Protocol Security
IRM. *See* information resource management
IRS. *See* U.S. Internal Revenue Service
IS. *See* information security
ISACA. *See* Information Systems Audit and Control Association
(ISC)². *See* International Information Systems Security Certification Consortium
ISMS. *See* information security management system
ISO. *See* International Organization for Standardization
ISO 27002
ISO/EIC 27001
ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27005

ISO/IEC JTC1
ISO/IEC standards
ISO technical committee
ISPs. *See* Internet service providers
ISSA. *See* Information Systems Security Association
ISSAF. *See* Information Systems Security Assessment Framework
IT. *See* information technology
IT asset AUP
IT Assurance Framework (ITAF)
IT audit process
IT auditing career opportunities
IT auditors
IT Governance
IT Governance Institute
IT infrastructure
IT infrastructure audit
IT infrastructure domains
IT security assessment
IT security audit
IT security employee job description
IT security policy
IT security policy framework
IT service delivery and support
IT universe
ITAF. *See* Information Technology Assurance Framework
ITGI. *See* Information Technology Governance Institute
ITL Bulletins. *See* Information Technology Laboratory Bulletins
ITU-T. *See* International Telecommunication Union Telecommunication Standardization Sector

J

job descriptions

K

Kerberos

L

LAN. *See* local area network
LAN Domain
LAN-to-WAN Domain
laptop computers
Layer 2 Forwarding (L2F)
Layer 2 switches
Layer 3 switches
Layer 2 Tunneling Protocol (L2TP)
layered audit approach
layered protocols
layered security
layers of controls
leadership
least privilege
L2F. *See* Layer 2 Forwarding
liability

likelihood determination process
local area network (LAN)
local printer
local resource
log review
logons
logs
L2TP. *See* Layer 2 Tunneling Protocol

M

MAC. *See* mandatory access control; Media Access Control
mainframe computers
maintenance procedures
malware
management controls
management tools and systems
mandatory access control (MAC)
mandatory vacation
MANs. *See* metropolitan area networks
maturity modeling
mechanism objects
Media Access Control (MAC)
Media Access Control (MAC) address
media storage plan
“Meeting Stakeholder Needs”
metro Ethernet
metropolitan area networks (MANs)
microcomputers
Microsoft Windows Server
minicomputers
misconfigurations
mission-critical data centers
MITRE Corporation
mixed WANs
Model Curricula for IS Audit and Control
monitoring
motivations
MPLS. *See* Multiprotocol Label Switching
multifactor authentication
multiple logons
Multiprotocol Label Switching (MPLS)

N

NAC. *See* Network Access Control
NAT. *See* network address translation
National Checklist Program (NCP)
National Do Not Call Registry
National Institute of Standards and Technology (NIST)
NCP. *See* National Checklist Program
NDA. *See* non-disclosure agreement
need to know basis
negotiation skills
Network Access Control (NAC)

network address translation (NAT)
network configuration management process
network device
network discovery
network documentation
Network Layer firewall
network management tools
network monitoring platforms (NMPs)
network operating system (NOS)
network performance
network port and service identification
network scan
network sniffing
network traffic monitoring device
networking devices
networking services software
New York Stock Exchange (NYSE)
NIST. *See* National Institute of Standards and Technology
NIST 800-30
NIST 800-53
NIST 800-53A
NIST 800-115
NIST Internal Reports (NISTIR)
NIST Special Publication 800-18
NIST Special Publication 800-30
NIST Special Publication 800-37
NIST Special Publication 800-39
NIST Special Publication 800-53
NIST Special Publication 800-53A
NIST Special Publication 800-59
NISTIR. *See* NIST Internal Reports
NMPs. *See* network monitoring platforms
nodes
non-disclosure agreement (NDA)
nongovernmental organizations
nonintrusive testing
noninvasive techniques
nonrepudiation
normative references, ISO/IEC 27001
NOS. *See* network operating system
NYSE. *See* New York Stock Exchange

0

object
objective setting, COSO framework
objectives
objectivity
objects
Office of Management and Budget (OMB)
ongoing assessment process
open issue tracking software
Open Source Security Testing Methodology Manual (OSSTMM)
Open Systems Interconnection (OSI) reference model
operating system
operating system patch management

operational audits
operational controls
operational impact
operations, ERM
operations security
optimization tools
organization-driven codes of conduct
organization of information security
organization-wide baseline
organizational policies
organizational records
organizational security policy framework
OSI reference model. *See* Open Systems Interconnection reference model
OSSTMM. *See* Open Source Security Testing Methodology Manual
owner

P

PA-DSS. *See* Payment Application Data Security Standard
packet-filtering firewall
packet sniffer
packet switching WAN
Paperwork Reduction Act of 1995
password cracking
patch management
Payment Application Data Security Standard (PA-DSS)
Payment Card Industry (PCI)
Payment Card Industry Data Security Standard (PCI DSS)
PCAOB. *See* Public Company Accounting Oversight Board
PCAOB Auditing Standard. *See* Public Company Accounting Oversight Board Auditing Standard
PCI. *See* Payment Card Industry
PCI DSS. *See* Payment Card Industry Data Security Standard
PDCA approach. *See* plan-do-check-act approach
penetration tests
pentester
performance accountability
performance management
performance measurement
performance monitoring
permissions
personal identification number (PIN)
personal information
Personal Information Protection and Electronic Documents Act (PIPEDA)
personally identifiable information (PII)
PHI. *See* protected health information
physical access controls
physical safeguards, HIPAA
physical security
PII. *See* personally identifiable information
PIN. *See* personal identification number
PIN Transaction (PTS) Security Requirements
PIPEDA. *See* Personal Information Protection and Electronic Documents Act
plan-do-check-act (PDCA) approach
Point-to-Point Tunneling Protocol (PPTP)
policies
power generator

power outages
PPTP. *See* Point-to-Point Tunneling Protocol
preproduction security assessment
prescriptive control framework
pretexting
preventive controls
PricewaterhouseCoopers (PwC)
principle of least privilege
print server
printer
Privacy Act of 1974
privacy audits
privacy data protection
privacy management
privacy officer
Privacy Rule
procedure
Process Capability Model
professional competence
professional ethics and integrity
“Professional Ethics and Standards Document #S3,”
project management
project management software
project plan
protected health information (PHI)
protocols
proxy server
PTS Security Requirements. *See* PIN Transaction Security Requirements
Public Company Account Reform and Investor Protection Act
Public Company Accounting Oversight Board (PCAOB)
Public Company Accounting Oversight Board (PCAOB) Auditing Standard
PwC. *See* PricewaterhouseCoopers

Q

QA. *See* quality assurance
Qualified Security Assessor (QSA)
quality assurance (QA)
quantitative risk analysis

R

RACI matrix
rack system
RADIUS. *See* Remote Authentication Dial In User Service
RANCID
reconnaissance
recovery plan
recovery strategy
Red Flags Rule
redundancy
redundant routers
regulatory agencies
regulatory compliance
regulatory requirements

remote access
Remote Access Domain
Remote Authentication Dial In User Service (RADIUS)
remote computer logon
remote connection process
remote devices
remote resource
remote service
remote users
remote workstations
removable media
removable storage devices
resistance
resource management
resources
responsibilities
responsibilities assignment
restore plan
results documentation process
review techniques
risk
risk appetite
risk assessment
risk-based approach
risk determination process
Risk IT
risk management
risk management framework (RMF)
risk management strategies
risk-mitigation strategies
risk response
risk tolerance
RMF. *See* risk management framework
rootkit
rotation of duties
round robin method
routers
ruleset review

S

Safeguards Rule
SAN. *See* storage area network
SANS Institute. *See* SysAdmin, Auditing, Network, Security Institute
SANS Technology Institute
SAQ. *See* self-assessment questionnaire
Sarbanes-Oxley (SOX) Act
SAS 70. *See* Statement on Auditing Standards 70: Service Organizations
SB1386
scanning
SCM. *See* security configuration management; software configuration management
scope creep
scope questions, ISACA
screening
SEC. *See* Securities and Exchange Commission
Secure Socket Tunneling Protocol (SSTP)

Secure Sockets Layer (SSL)
Secure Sockets Layer/Transport Layer Security (SSL/TLS)
secure VPNs
Securities and Exchange Commission (SEC)
security assessment techniques
security assessments
security audit
security awareness
security baseline
security compliance audit
security configuration management (SCM)
security controls
security guidelines
security incident management
security management
security operation policies
security operations
security policies
security policy framework
security procedures
security-related activities
Security Rule
security standards
security training
segregation of duties
self-assessment questionnaire (SAQ)
“Separating Governance from Management.,”
separation of duties
server computers
Server Message Block (SMB)
service audit reports
service identification, network port and
service level agreements (SLAs)
Service Organization Control (SOC) reports
service organizations
service providers
services
services devices
Shewhart cycle
shielded twisted pair (STP) cable
Simple Network Management Protocol (SNMP)
single points of failure
single router
single router with backup
skills required, ISACA
SLAs. *See* service level agreements
smartphones
SMB. *See* Server Message Block
SMSPI. *See* Social Media Security Professional
SNMP. *See* Simple Network Management Protocol
SOC 1
SOC 2
SOC 3
SOC reports. *See* Service Organization Control reports
social engineering
social engineering testing

Social Media Security Professional (SMSP)
Social Security number (SSN)
SoftSea Remote Access Monitor
software configuration management (SCM)
software development and maintenance
source code
SOX Act. *See* Sarbanes-Oxley Act
Special Publications from NIST
specification object
spyware
SSCP. *See* Systems Security Certified Practitioner
SSL. *See* Secure Sockets Layer
SSL/TLS. *See* Secure Sockets Layer/Transport Layer Security
SSN. *See* Social Security number
SSTP. *See* Secure Socket Tunneling Protocol
standard control framework
standards
Statement on Auditing Standards 70: Service Organizations (SAS 70)
Statement on Standards for Attestation Engagements No. 16 (SSAE 16)
statutes
storage area network (SAN)
STP cable. *See* shielded twisted pair cable
strategic, ERM
structured shutdown
subject
subnets
summary of finding
surge protection
switches
SysAdmin, Auditing, Network, Security (SANS) Institute
System/Application Domain
system characterization process
system connection encryption
system security plan
Systems and Infrastructure Life Cycle Management
Systems Security Certified Practitioner (SSCP)

T

tablet devices
tablets
TACACS+. *See* Terminal Access Controller Access-Control System Plus
target vulnerability validation techniques
TCP/IP. *See* Transmission Control Protocol/Internet Protocol
TCP/IP reference model
TDE. *See* Transparent Data Encryption
technical controls
technical safeguards, HIPAA
temporary behavior
Terminal Access Controller Access-Control System Plus (TACACS+)
test method
testing and quality assurance (QA)
testing security controls
threat
threat actions
threat identification

threat likelihood
threat statement
time
time to recover (TTR)
TJX Companies, Incorporated
TLS. *See* Transport Layer Security
TLS VPN Remote Access
tokenization
traffic monitoring
traffic-monitoring devices
training
Transmission Control Protocol (TCP)
Transmission Control Protocol/Internet Protocol (TCP/IP)
Transmission Control Protocol/Internet Protocol (TCP/IP) reference model
transmission encryption
Transparent Data Encryption (TDE)
Transport Layer Security (TLS)
triple constraint
Trojan horse
TTR. *See* time to recover
tunneling
two-factor authentication
Type 1 report
Type 2 report
Type I authentication (what you know)
Type II authentication (what you have)
Type III authentication (what you are)

U

UDP. *See* User Datagram Protocol
unauthorized systems and software
Unified Framework of Professional Ethics for Security Professionals
uninterruptible power supply (UPS)
universal serial bus (USB) drive
unshielded twisted pair (UTP) cable
UPS. *See* uninterruptible power supply
URL filter
U.S. compliance laws
U.S. Department of Defense (DoD) requirements
U.S. Department of Health and Human Services (HHS)
U.S. Internal Revenue Service (IRS)
USB drive. *See* universal serial bus drive
User Datagram Protocol (UDP)
User Domain
user entities
user interface
users
UTP cable. *See* unshielded twisted pair cable

V

val IT framework
vendor-neutral certifications
virtual machines

virtual private networks (VPNs)
virus
volume/drive encryption
VPNs. *See* virtual private networks
vulnerabilities
vulnerability analysis
vulnerability identification process
vulnerability management
vulnerability scan

W

WAN. *See* wide area network
WAN access device
WAN account
WAN Domain
WAN optimization device
WAN optimizers
WAN service providers
wardialing
wardriving
warm site
web application
web content filtering device
Web server
WEP. *See* Wired Equivalent Privacy
white-box testing
Wi-Fi Protected Access (WPA)
wide area network (WAN)
wide area network (WAN) service provider
Windows Group Policy Management Editor
Wired Equivalent Privacy (WEP)
wired LAN connections
wireless
wireless access points
wireless LAN connections
wireless local area network (WLAN)
wireless scanning
WLAN. *See* wireless local area network
Workstation Domain
workstation vulnerability management
WorldCom
worm
WPA. *See* Wi-Fi Protected Access