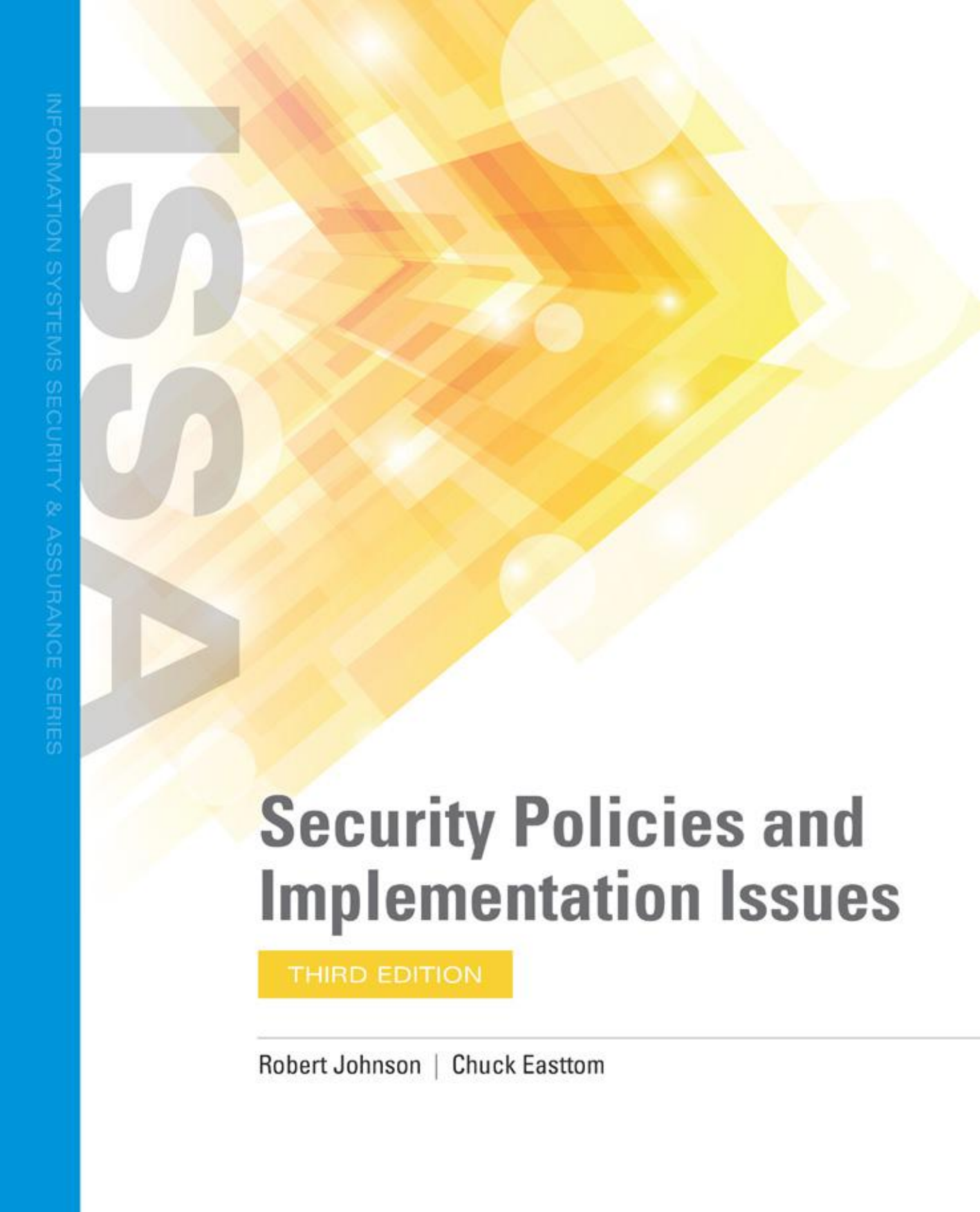


Security Policies and Implementation Issues

THIRD EDITION

Robert Johnson | Chuck Easttom

INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Security Policies and Implementation Issues

THIRD EDITION

Robert Johnson | Chuck Easttom

JONES & BARTLETT
LEARNING

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.

Production Credits
VP, Product Management: Amanda Martin
Director of Product Management: Laura Pagluica
Product Manager: Edward Hinman
Content Strategist: Melissa Duffy
Content Coordinator: Paula-Yuan Gregory
Development Editor: Ginny Munroe
Technical Editor: Rob Shimonski
Project Manager: Lori Mortimer
Project Specialist: John Coakley
Digital Project Specialist: Rachel DiMaggio
Marketing Manager: Michael Sullivan
Production Services Manager: Colleen Lamy
Product Fulfillment Manager: Wendy Kilborn
Composition: Exela Technologies
Project Management: Exela Technologies
Cover Design: Briana Yates
Text Design: Kristin E. Parker
Media Development Editor: Faith Brosnan
Rights Specialist: James Fortney
Cover Image (Title Page, Part Opener, Chapter Opener): © obpcnh/Shutterstock
Printing and Binding: LSC Communications

Library of Congress Cataloging-in-Publication Data
Names: Johnson, Rob (Robert), author. | Easttom, Chuck, author.
Title: Security policies and implementation issues / Robert Johnson, Chuck Easttom.
Description: [Third edition] | Burlington, MA : Jones & Bartlett Learning, [2021] | Includes bibliographical references and index.
Identifiers: LCCN 2020018594 | ISBN 9781284199840 (paperback)
Subjects: LCSH: Computer security.
Classification: LCC QA76.9.A25 J64 2021 | DDC 005.8–dc23
LC record available at https://lccn.loc.gov/2020018594

6048

Printed in the United States of America

24 23 22 21 20 10 9 8 7 6 5 4 3 2 1

Brief Contents

Contents

To my wife Teresa, who is always very supportive of all I do.
—Dr. Chuck Easttom

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 Certified Information Systems Security Professionals (CISSPs), they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but forward thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow, as well.

Implementing IT security policies and related frameworks for an organization can seem like an overwhelming task, given the vast number of issues and considerations. *Security Policies and Implementation Issues* demystifies this topic, taking you through a logical sequence of discussions about major concepts and issues related to security policy implementation.

It is a unique book that offers a comprehensive, end-to-end view of information security policies and frameworks from the raw organizational mechanics of building to the psychology of implementation. This book presents an effective balance between technical knowledge and soft skills, both of which are necessary for understanding the business context and psychology of motivating people and leaders. It also introduces you in clear, simple terms to many different concepts of information security, such as governance, regulator mandates, business drivers, legal considerations, and more. If you need to understand how information risk is controlled, or are responsible for oversight of those who do, you will find this book helpful.

Part 1 of this book focuses on why private and public sector organizations need an information technology (IT) security framework consisting of documented policies, standards, procedures, and guidelines. As businesses, organizations, and governments change the way they operate and organize their overall information systems security strategy, one of the most critical security controls is documented IT security policies.

Part 2 defines the major elements of an IT security policy framework. Many organizations, under recent compliance laws, must now define, document, and implement information security policies, standards, procedures, and guidelines. Many organizations and businesses conduct a risk assessment to determine their current risk exposure within their IT infrastructure. Once these security gaps and threats are identified, design and

implementation of more-stringent information security policies are put in place. This can provide an excellent starting point for the creation of an IT security policy framework.

Policies are only as effective as the individuals who create them and enforce them within an organization. Part 3 of this book presents how to successfully implement and enforce policies within an organization. Emerging techniques and automation of policy enforcement are also examined.

This book is a valuable resource for students, security officers, auditors, and risk leaders who want to understand what a successful implementation of security policies and frameworks looks like.

Learning Features

The writing style of this book is practical and conversational. Step-by-step examples of information security concepts and procedures are presented throughout the text. Each chapter begins with a statement of learning objectives. 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.

New to This Edition

- Covers additional standards:
  - ISO 38500
  - ISO 27007
  - ISO 30105
  - GDPR
  - ETSI
- Updated NIST Special Publication (SP) 800-53 for the 2019 changes
- Updated COBIT for COBIT 2019
- Added the CIS Critical Security Controls for Effective Cyber Defense
- Added coverage of mobile devices in the workplace (BYOD, COPE, CYOD)
- Included additional models like McCumber Cube
- Updated statistics and case studies

Theory Labs

This text is accompanied by Cybersecurity Theory Labs. These hands-on labs provide guided exercises and case studies where students can learn and practice foundational cybersecurity skills as an extension of the lessons in this textbook. For more information or to purchase the labs, visit go.jblearning.com/johnson3e

Acknowledgments

We would like to thank Jones & Bartlett Learning for the opportunity to work on this book and be a part of the Information Systems Security & Assurance Series project. It is always a pleasure to work with a high-quality publisher who pushes for the best book they can create.

About the Authors

ROB JOHNSON has more than 22 years of experience in information risk, IT audit, privacy, and security management. He has a diverse background that includes hands-on operational experience, as well as providing strategic risk assessment and support to leadership and board-level audiences. He is currently a Senior Vice President at Bank of America in the Global Technology Organization.

Johnson has held senior roles in large global companies, in large domestic banks, and as product architect for an international software company. Several of the key risk-related roles he has held include Head of Information and Operations Risk Management for ING U.S. Financial Services, Senior Partner at Aegis USA Executive Consulting, First Vice President and IT Senior Audit Director for WAMU, Vice President/CISO for Security Services at First Bank Systems, and Product Owner and Architect for SAP/ERP solutions at Bindview.

Johnson lives in the Seattle area with his wife and children. He holds a BS in interdisciplinary studies from the University of Houston with a concentration in computer science and mathematics. He is a Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), and Certified in the Governance of Enterprise IT (CGEIT). Rob has served on several international education and standards committees, including as 1 of 19 former members of the prestigious international C5 Task Force that developed COBIT 2019.

DR. CHUCK EASTTOM is the author of 29 books, including several on computer security, forensics, and cryptography. His books are used at over 60 universities. He has also authored scientific papers (over 60 so far) on digital forensics, cyber warfare, cryptography, and applied mathematics. He is an inventor with 22 computer science patents. He holds a Doctor of Science (DSc) in cyber security (dissertation topic: "A Study of Lattice-Based Cryptographic Algorithms for Post Quantum Computing") and three master's degrees (one in applied computer science, one in education, and one in systems engineering). He also holds a Doctor of Philosophy (PhD) in nanotechnology. and is currently working on a PhD in computing from the University of Portsmouth (dissertation topic: "On the Application of Algebraic Graph Theory to Network Forensics"). He is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE) and a Senior Member of the Association of Computing Machinery (ACM). He is also a Distinguished Speaker of the ACM, a Distinguished Visitor of the IEEE Computer Society, and a frequent speaker at conferences. He is a reviewer for six scientific journals and the Editor in Chief for the American Journal of Science and Engineering. He also currently holds 55 industry certifications (CISSP, CASP, CEH, etc.). More details are available at www.ChuckEasttom.com

PART ONE

The Need for IT Security Policy Frameworks

CHAPTER 1

Information Systems Security Policy Management

FOR AN ORGANIZATION TO ACHIEVE ITS GOALS, business processes must be reliable, affordable, and legal. Reliable policies require clearly defined processes. Most organizations use policies and procedures to tell employees what the business wants to achieve and how to perform tasks to get there. This way, the business can achieve consistent quality in delivering its products and services.

Though policies and procedures need to be reliable, affordable, and legal, policies are not perfect. Even if a policy is inherently perfect, perfect implementation of it would require employees to follow policies and procedures at all times; however, we do not live in a perfect world. Neither policies nor procedures are always perfect, nor do employees always follow them. Anyone who has cashed a check at a bank understands what a basic procedure looks like. A check-cashing procedure includes checking the person's identification and the account balance. The bank's policy states that when a teller follows the check-cashing procedure and the account has sufficient funds, the teller may give the cash to the account holder. The teller must follow this procedure to protect the customer and the bank from fraud. Failure to do so can be a substantial breach and can have significant deleterious consequences.

Business processes are highly dependent on timely information. It's also challenging to find an organization that does not rely on technology, whether it sells hamburgers, cashes checks for people, or is building the next-generation airliner. Processes use technology and information to make business decisions, keep food safe, track inventory, and control manufacturing, among other things. The more complex these technologies become, the more vulnerable they become to disruptions. The more people rely on them in their daily lives, the more vulnerable they become when these technologies do not work.

You can also think of a policy as a business requirement of actions or processes performed by an organization. An example is the requirement that a customer provide a receipt when returning an item to a retail store for a refund. That may be a simple example, but essentially, it places a control on the return process. In the same manner, security policies require placement of controls in processes specific to the information system.

One of the challenges organizations face is the cost of keeping pace with ever-changing technology. This includes the need to update policies at the same time the organization updates technology. Failure to do so can create weaknesses in the system. These weaknesses make business processes and information vulnerable to loss or theft.

Many factors drive the policy requirements of **information systems security policies**, also called *security policies*, *IS policies*, or *ISS policies*. These requirements include the organization's size,

processes, the types of information the business deals in, and the laws and regulations that may affect the policies. Once an organization creates policies, it will face both technical and human challenges implementing them. The keys to implementing policies are employee acceptance and management enforcement. A policy is worth little or nothing if no one follows it.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- What information systems security is
- How information assurance plays an important role in securing information
- What governance is
- Why governance is important
- What information systems security policies are and how they differ from standards and procedures
- Where policies fit within an organization's structure to effectively reduce risk
- Why security policies are important to business operations, and how business changes affect policies
- When information systems security policies are needed
- Why enforcing, and winning acceptance for, security policies is challenging

Chapter 1 Goals

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

- Compare and contrast information systems security and information assurance
- Compare and contrast quality control and quality assurance
- Describe information systems security policies and their importance in organizations
- Describe governance and its importance in maintaining compliance with laws
- Explain what policies are and how they fit into an organization
- Compare and contrast threats, vulnerabilities, and risks

What Is Information Systems Security?

A good definition of **information systems security (ISS)** is the act of protecting information and the systems that store and process it. This protection is against risks that would lead to unauthorized access, use, disclosure, disruption, modification, or destruction of information. The first thing that should be clear from this definition is that ultimately it is the information that requires protecting. Usually, information is on digital devices

such as computers, tablets, routers, and similar devices. Those devices' primary value is the information on them.

It is important to remember that it is not just the information inside a computer you need to protect. Information needs to be protected in any form. Some examples include print and removable storage such as optical DVD drives. In fact, well-structured security policies ensure protection of information in any location and in any form. Many organizations come up with effective ways of protecting buildings, people, and other physical resources. Most people understand the need to lock their doors at home at night. Yet they may not always have the same instincts or habits when it comes to handling their data.

Sometimes the rules for dealing with information are unclear. Suppose your business knows a person's name, phone number, and email address. How much privacy should that person expect from your business? What are you obligated by law to protect? What's the right thing to do ethically? These are just some of the questions businesses struggle with daily. Not every employee is an expert in these matters. So, organizations create policies and procedures for their employees to follow.

Sometimes these same organizations fail to properly protect the information they process. Some do not consider information important to their operations. Some believe that security measures designed to protect buildings and people will protect information. Some just do not want to spend more money. However, protecting information is vital to business operations.

Information Systems Security Management Life Cycle

Generally, in any process of importance, you would use some type of life cycle process to reduce errors and make sure all requirements are considered. It is no different for implementing security policies. Information security controls and processes use common approaches that simplify the build and reduce mistakes. A typical life cycle process breaks up tasks into smaller, more manageable phases. The Information Systems Audit and Control Association (ISACA) developed a widely accepted international best practices framework. This framework, called Control Objectives for Information and related Technology (COBIT), was first released in 1996. The next major version, 5.0, was released in April 2012. This version is still in use; however, in 2018, COBIT 2019 was released. COBIT 2019 includes:

- Design factors and focus areas that offer more transparency on building a governance system
- Improved compliance with global frameworks
- Consistent updates on a rolling basis
- An open-source model that enables feedback from the external governance community for quicker enhancements
- Better instructions and a broader toolkit to assist enterprises with creating a top-notch governance system
- An improved tool for measuring Capability Maturity Model Integration (CMMI) alignment and IT performance
- Greater support for decision making

COBIT 2019 is made up of the following elements that differentiate it from previous versions of COBIT:

- Design factors and focus areas that offer more transparency on building a governance system
- Improved compliance with global frameworks
- Consistent updates on a rolling basis
- An open-source model that enables feedback from the external governance community for quicker enhancements
- Better instructions and a broader toolkit to assist enterprises when creating a top-notch governance system
- An improved tool for measuring CMMI alignment and IT performance
- Greater support for decision-making

COBIT is more than just a life cycle; it's a framework for managing and governing IT processes. These types of frameworks allow businesses to align themselves to outcomes that they and their customers expect. At its core are four domains that collectively represent a conceptual **information systems security management life cycle**:

- Align, Plan, and Organize
- Build, Acquire, and Implement
- Deliver, Service, and Support
- Monitor, Evaluate, and Assess

NOTE

You can read more about COBIT at *https://www.isaca.org/resources/cobit*.

The life cycle process can use these simple domains, or phases, to build policies or controls. Each phase builds on the other. A failure in one phase can lead to a weakness or vulnerability downstream. For the purposes of discussion, you will learn about the four domains from a high-level life cycle view. The COBIT framework goes into great depth to further break down these domains into detailed tasks and processes. Many organizations look at the richness of a framework like COBIT to tailor a life cycle management approach that makes sense for their business.

In 2012, COBIT 5.0 was released to the public. This version of COBIT introduced the idea that good business processes make it possible for organizations to do the following:

- Deliver value to internal and external stakeholders.
- Meet organizational goals.
- Practice life cycle management: building, maintaining, supporting, and disposing of products and other assets.
- Learn from others to keep abreast of industry best practices.

COBIT 5.0 was a departure from other frameworks in that it put emphasis on what enables processes to work well. In fact, COBIT calls these *process enablers*. For example, think of a teller cashing a check. What does a bank have to think about to align, plan, and organize to achieve stakeholder value? Clearly the bank wants the customer, as the external stakeholder, to have a good experience. This will build loyalty and repeat business. But the customer needs must be balanced with the business goal of making a

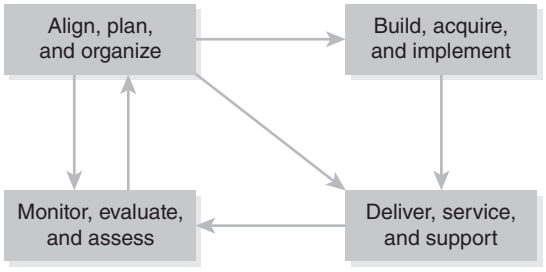


FIGURE 1-1
A simplified ISS management life cycle using COBIT 5.0.

profit. The bank must also be aware of changing industry standards and new technology such as mobile devices.

As was already discussed, COBIT 2019 expanded and built on COBIT 5.0, but most of the fundamentals remain.

FIGURE 1-1 depicts one simplified example of an ISS management life cycle.

Align, Plan, and Organize

The COBIT Align, Plan, and Organize domain includes basic details of an organization's requirements and goals. This domain answers the questions "What do you want to do?" and "How do you want to get there?" The information in this phase is still high level. Even at a high level, it is important to understand the risks and threats clearly. You review how you are going to manage your IT investment such as contracts, **service level agreements (SLAs)**, and new policy ideas. An SLA is a stated commitment to provide a specific service level. For example, an SLA could state how often a supplier will provide the service or how quickly the firm will respond. For managed services, the SLA often covers system availability and acceptable performance measures. It's also important to look at where or how the system will operate to determine the SLA. SLAs are important to ensure that all parties know their obligations. There are different types of service levels that apply to contracts versus what you need to deal with day to day. The Deliver, Service, and Support domain helps you define and manage day-to-day SLAs. In the Align, Plan, and Organize domain, you are primarily concerned with the type of equipment and services you are acquiring and how to hold a supplier accountable for those deliveries.

NOTE

Notice in Figure 1-1 that the Align, Plan, and Organize domain touches all the other domains. This is because you will determine how the project will be managed in the Align, Plan, and Organize domain. This means you need to initially decide and then adjust management and staff throughout the project.

A contract must provide the ability to ensure a supplier meets its obligations. The SLA language in a contract must provide clear monitoring and enforcement rights. For example, consider the 2013 breach of Target stores. Although this is an older breach, it is one of the major events in cybersecurity history and still worthy of consideration. Between November 27 and December 15, 2013, hackers accessed the credit card information of 40 million customers. Later it was discovered that an additional 70 million customers' personal information was also accessed by hackers. It's been widely reported the hacker gained access through the supplier who maintained the company's heating and air conditioning systems. Simply having a contract with the supplier wasn't enough. Target had an obligation both to limit the supplier's access while on its network and to monitor access

sufficiently to ensure the contract was being enforced. These are general industry norms. Either one or both of these did not occur.

A key understanding in this life cycle phase is the understanding of threats, vulnerabilities, and risks. These three concepts are addressed in different forms throughout this text; however, a basic understanding is essential to scope the build effort. To understand these concepts, consider the following high-level definitions:

- **Threat**—A human-caused or natural event that could impact the system
- **Vulnerability**—A weakness in a system that can be exploited
- **Risk**—The likelihood or probability of an event and its impact

As an example, a common IS **threat** would be a hacker trying to break into a system. A **vulnerability** would be a weakness in a system that allows the hacker to gain unauthorized access. A vulnerability could be a misconfiguration, bug, or flaw in the system. A **risk** is a combination of the likelihood that such a misconfiguration could happen, a hacker's exploiting it, and the impact if the event occurred. Consider a non-Internet-facing system for ordering office supplies. Why might you think the risk is low? Although a misconfiguration may be possible, systems not on the Internet are less likely to be hacked. Additionally, unauthorized access to the office supply system would most likely have little long-term impact on a company.

> **NOTE**
>
> Generally, regardless of threat or vulnerability, there will always be a chance a threat can exploit a vulnerability. Consequently, whenever you have a threat or vulnerability, you will have a risk. The key is understanding whether that risk is small (unlikely) or large (probable).

Other examples may be of higher risk and require significant investment. An example of a natural threat would be a hurricane. A vulnerability may be a lack of a recovery site. If your main data center, for example, is damaged, where would you go? The risk may be high for a business that relies on Internet orders, especially if the business is located in Florida, which is prone to hurricanes.

Build, Acquire, and Implement

The COBIT Build, Acquire, and Implement domain addresses schedules and deliverables. The basic build occurs within this phase. The *build* is where the security control is built and policies and supporting documents written. The build is based on the requirement created in the Align, Plan, and Organize phase. The quality of the security controls that are built depends on the understanding of the threats, vulnerabilities, and risks. The deeper this understanding, the better the controls. The more detailed the requirements, the more easily the build will go. The more details included in the Align, Plan, and Organize phase, the easier the Build, Acquire, and Implement phase will be. The SLA becomes an important consideration of the build because it determines the type of solutions that will be selected.

Additionally, the ability to manage change is critical in this phase. Often, changes known as *upgrades* are made to existing systems. That means changes have to be timed perfectly. This is to avoid disrupting current services while new services are added. Often this will occur during off-hours such as weekends or overnight. Plans have to be put in place to back out the change in the event of a major problem. Understanding the impact of change and knowing how to recover if something goes wrong are parts of **change management**.

By the end of the Build, Acquire, and Implement phase, you have acquired and implemented your equipment. You have controls built into the systems. You have policies, procedures, and guidelines written. You have teams trained.

Deliver, Service, and Support

In the COBIT Deliver, Service, and Support domain, the staff tunes the environment to minimize risks. It is in this phase that you collect lessons learned. By running the systems, you learn what's working and what isn't. This is where you apply those lessons learned to improve operations. This could mean adjusting controls, policies, procedures, contracts, and SLAs. It is here you analyze data from the prior phase and compare it with day-to-day operations. You also perform internal and external penetration testing and, based on the results of those tests, make critical adjustments in areas such as perimeter defense, remote access, and backup procedures. You review contracts and SLAs for validity and modify them as needed.

This phase requires regular meetings and good communication with your vendors. You must quickly identify any issues with the vendors' capabilities to meet SLAs. Typically, a vendor provides its record for meeting SLAs. You compare the vendor's report to your organization's internal reports. If you rely heavily on the vendor, you should meet monthly to compare records and recap incidents during the month. It is important that SLAs also be explicit. Failure to clarify precisely what services are provided and how they are provided can lead to confusion and dissatisfaction from both the customer and the vendor.

In this phase, the day-to-day operations are managed and supported. You manage problems, configurations, physical security, and more. If you plan correctly and implement the right solution, your organization sees value.

Monitor, Evaluate, and Assess

After evaluating the ISS management life cycle, you can see that ISS focuses on specific types of controls at specific points within the system. Testing and monitoring of controls occur, and the results are analyzed for effectiveness. The oversight of the COBIT Monitor, Evaluate, and Assess domain looks at the big picture. Are your controls and supporting policies and procedures keeping pace with changes in technology and in your environment? This phase looks at specific business requirements and strategic direction and determines whether the system meets these objectives.

Internal and external audits occur during the evaluation phase. Audits also take place through all testing in this and prior phases to ensure requirements are being met. This may include penetration testing by a third-party trusted agent. The testing performed during this phase must be comprehensive enough to encompass the entire ISS environment. The level of additional security testing will depend on business requirements and complexity; for example, if your requirements include regulatory compliance, include appropriate control tests. You should also evaluate the incident response process.

Audits are independent assessments. The more robust the self-assessment process, the fewer the problems that will be discovered by an audit. Independence is a relative term. No one is truly independent. Consider this: Everyone belongs to a family. Everyone lives in a town or city. Everyone has a multitude of private and business relationships. People may feel comfortable criticizing politicians but suddenly uncomfortable criticizing a teacher who has the power over their final grade. It's human nature that the closer the relationship, or

the more control someone has over your well-being, the less likely you are to criticize. Yet in business, this honest view of mistakes is essential to success.

The concept of independent audits (or assessments) is that the further one is away from the actual transaction, the more unbiased and independent the opinion that can be obtained. In other words, it's hard to criticize your own work. However, the more you understand the work, the better your chances are, generally, of finding out what went wrong. To balance these potentially competing interests, there is usually a series of assessments and audits. The following lists the most common types of assessments and audits:

- **Self-assessment**—This is typically in the form of quality assurance (QA) and quality control (QC).
- **Internal audit**—This consists of reports to the board of directors and assesses the business.
- **External audit**—This is done by an outside firm hired by the company to validate internal audit work and perform special assessments, such as certifying annual financial statements.
- **Regulator audit**—This is an audit by government agencies that assess the company's compliance with laws and regulations.

ISO/IEC 38500

Although COBIT is widely used and respected, it is not the only standard relevant to the information systems security management life cycle. The International Standards Organization publishes ISO 38500, "Information Technology—Governance of IT for the Organization," which provides guidance for managing IT governance. This standard is broader than just information systems security, but it includes and is applicable to information systems security management.

This standard was last revised in 2015. It specifically addresses monitoring of resources and auditing, both of which are clearly information systems management functions. This framework sets out six principles for corporate governance of information technology:

- Responsibility
- Strategy
- Acquisition
- Performance
- Conformance
- Human behavior

Clearly, each of these is as applicable to information security systems as it is to IT in general.

What Is Information Assurance?

Too often you will hear the terms *information systems security* and *information assurance* used interchangeably; however, they are not the same thing. **Information assurance (IA)** grew from information systems security. The high-level difference is that ISS focuses on protecting information regardless of form or process, whereas IA focuses on protecting information

during process and use. You can see some of these differences as you examine the security tenets, also known as the "five pillars of the IA model":

- **Confidentiality**—Generally accepted as ISS and IA tenets
- **Integrity**—Generally accepted as ISS and IA tenets
- **Availability**—Generally accepted as ISS and IA tenets
- **Authentication**—Generally accepted as an IA tenet
- **Nonrepudiation**—Generally accepted as an IA tenet

The first three—confidentiality, integrity, and availability—are bedrock principles throughout information security. These are often referred to as the *CIA triangle*. (Some sources refer to this as the *CIA triad*; the two terms are synonymous.) This is not to suggest that authentication and nonrepudiation are not information security concerns. The goals are similar; however, the approach and focus are different. IA imposes controls on the entire system regardless of the format or media. In other words, IA ensures data is protected while being processed, stored, and transmitted. This ensures the confidentiality, integrity, availability, and nonrepudiation of the data.

Confidentiality

Confidentiality is the goal of ensuring that only authorized individuals are able to access information. A user should be granted access only to the specific information necessary to complete his or her job.

Typical users do not need unlimited access to all systems and all data. In fact, in regulated environments, if ordinary users had such access, this would be viewed as a compliance issue and a violation of law. Many organizations have adopted the **need-to-know principle**. In brief, this means that you gain access only to the systems and data you need to perform your job. For example, payroll personnel may need your employee and personal information, such as salary and Social Security number. Your manager may need access to your salary for budgeting but not your Social Security number. By restricting access, you maintain confidentiality.

FIGURE 1-2 depicts the confidentiality tenet. The figure represents three users—two are regular users; one is a privileged user. User A and User B have limited access rights to data. User A can read only data stored in the product list, whereas User B can read and update all data in the database. The privileged user has elevated database administration privileges; however, even he or she might not have access to all data.

NOTE

Another consideration of confidentiality is how to protect data in the event of a breach or unauthorized access. One way to resolve this issue is to use encryption. This is considered a security layered approach. A breach in one layer will be caught by another. In this case, even if data is improperly accessed, it still cannot be read.

Integrity

Integrity ensures that information has not been improperly changed. In other words, the data owner must approve any change to the data or approve the process by which the data changes. There are several ways to ensure that data is protected. Many operating systems allow permissions on data files and directories to provide restricted access. These

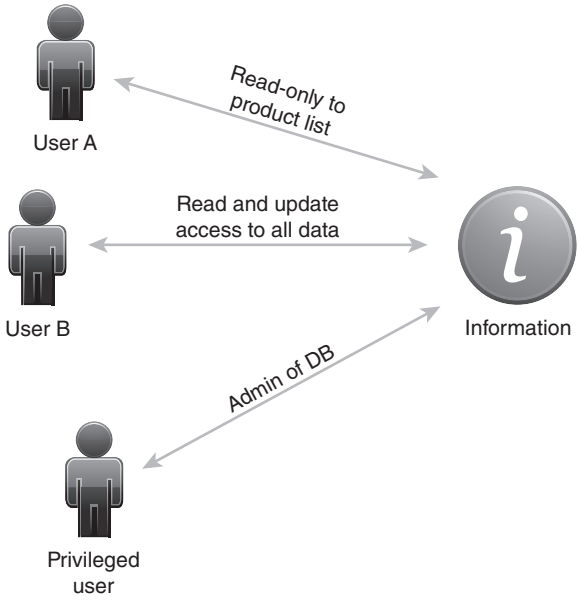


FIGURE 1-2
The confidentiality tenet.

containers typically reside on a server that requires users to log on and authenticate to gain approved access. This ensures that only users who have the data owner's permission can change the information. Often, access is limited to an application. In this way, a user does not access data directly. The user accesses the application. The application accesses the data. So, the application acts as a gateway. This allows for more fine-grained granting of access, often referred to as **entitlement**. With entitlement, you can restrict the type of access a user has. For example, the application can allow a user to approve a payment but limit the amount to less than $1000. Encryption also ensures integrity as well as confidentiality. Encryption protects data from being viewed or changed by unauthorized users. Only users with the proper key can change or view encrypted data. Encryption is often used to protect data being transmitted or moved. Encryption can also be used to protect data at rest.

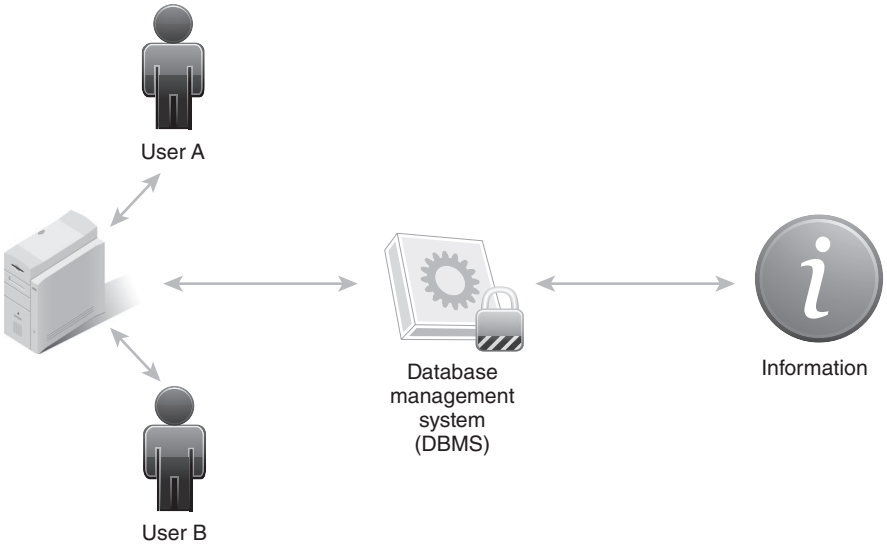
FIGURE 1-3 depicts the integrity tenet. There are two users, an application, a database management system (DBMS), and the data. The application control limits the type of change a user can make. The DBMS rules prevent unauthorized changes to data. User A can change data. User B can only retrieve data.

Authentication

Authentication is the ability to verify the identity of a user or device. You probably see authentication in use every day. For example, you might use an online email system such as Google Gmail or Yahoo! Mail. What protects your email is your user ID and password, which you selected when you signed up for the service. This user ID and password are your authentication approach to accessing your email service.

It's not just humans who need their identities verified. Computers often exchange information or process transactions on our behalf. While you are asleep, a computer system may by printing your payroll check. Many of these functions are sensitive. As a security professional, you should ensure that only these authorized processes are accessing this sensitive

FIGURE 1-3
The integrity tenet.



information. This means these computers and automated processes need to be authenticated. Just like an individual, their identity is verified before being granted access to data. For example, services running in Microsoft Windows Server could have an ID assigned. Network devices can exchange information at a network protocol level to verify identity. These nonhuman IDs typically have elevated rights. This means they have lots of authority to access data across multiple systems. It's important that access to these nonhuman accounts be tightly controlled.

There is a lot involved in maintaining good authentication processes, such as forcing users to change their passwords periodically and forcing rules on how complicated passwords should be. These housekeeping tasks are becoming easier and more automated. One of the more critical keys to success is having credentials that are hard to forge or guess. A good example is a strong password known only to the user. Additionally, these credentials must not be transmitted in the clear over the network. Passwords sent over the network in plaintext, for example, can be observed with network sniffers. In a typical business environment, if these two goals are accomplished as well as many of the housekeeping items previously discussed, you begin to have reasonable assurance you know who is accessing your computer systems.

Availability

Availability ensures information is available to authorized users and devices. A major challenge to availability is the spread of *denial of service (DoS) attacks*. The technological sophistication and intensity of DoS attacks have increased significantly in recent years. These attacks flood a server with information that overwhelms its ability to process, causing the server to crash. Thus, the service becomes unavailable. The point of the attack is not to steal information but to crash the system. DoS attacks are often measured by the amount of information

flooding the server. The typical measurement is in Gbps (gigabits per second). The size of DoS attacks keeps growing. In 2018, it was reported that the average DoS attack was bigger than 26 Gbps, and the maximum attack size was 359 Gbps.[1] However, in 2019, the average size decreased by 85 percent, and the maximum attack size decreased by 24 percent.[2]

Initially, the information owner must determine availability requirements. The owner must determine who needs access to the data and when. Is it critical that data be available 24/7, or is 9 to 5 adequate? Does it need to be available to remote or only local users? The raw business requirements then need to be translated into technical and operational commitments, such as hours of operations for when the systems would be available.

After availability requirements are determined, you must assess the threats and implement appropriate controls. Associated with the servers is all the network equipment that provides interconnectivity and remote access. Proper configuration of these devices will allow access to the information when needed.

Nonrepudiation

Nonrepudiation is both a legal term and a concept within information security. The idea is simple—nonrepudiation is the assurance that an individual cannot deny having digitally signed a document or been party to a transaction. As a legal concept, it is the sum total of evidence that proves to the court's satisfaction that only one person could have executed that transaction.

Before the Internet, individuals struggled with the question. When you sign a legal document, often you need a notary. That notary is there to be part of the nonrepudiation process of gathering evidence. He or she takes copies of your identification and matches signatures. Some even take a thumbprint. All this effort is so that later you cannot claim it wasn't you who signed.

So how do you sign a document electronically? A leading method is to use a digital signature. If used properly, the electronic signature cannot be forged and is digitally timestamped. Most important, the receiver of the document can verify it is your digital signature. But even a digital signature relies on a private key that must be protected. It's worth noting that these digital signatures are legally binding under the U.S. Federal ESIGN Act of 2000.

However, many final electronic transactions do not use digital signatures. In fact, often online banking transactions, money transfers, or buying and selling stock rely on other technology, including strong authentication. Ultimately you want to prove that only that person could have executed that transaction. A leading vendor in this space is IBM, whose flagship product for secure messaging is called Websphere. IBM defines nonrepudiation as an end-to-end service that "can be viewed as an extension to the identification and authentication service." Although secure messaging ensures the collection and delivery of the transaction, the application that consumes the message still has to be proven as secure.

It should be noted that the CIA triangle, although widely used in information security, is a somewhat simplistic model, and there have been expansions to it. The McCumber cube is one such expansion of the CIA triangle that is worth discussing. It was described in detail in 2004 in the book *Assessing and Managing Security Risk*

NOTE

The Federal ESIGN Act defines an electronic signature as an "electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." To learn more, go to *https://www.fdic.gov/regulations/compliance/manual/10/x-3.1.pdf*.

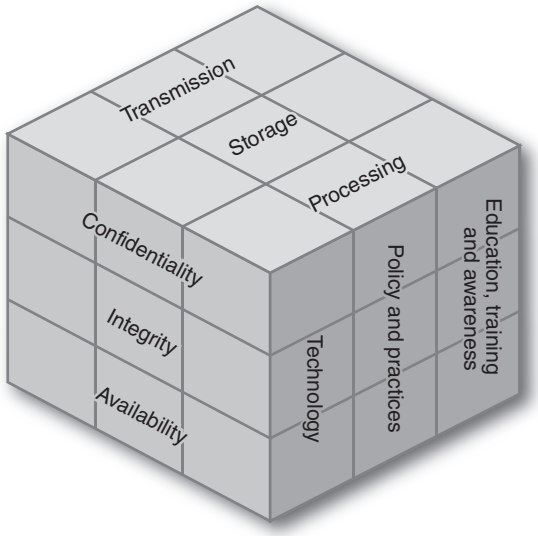


FIGURE 1-4
The McCumber cube.

in IT Systems: A Structured Methodology. It looks at security as a three-dimensional cube. The concept is to add more dimensions to the traditional CIA triangle. In addition to the three aspects of the CIA triangle, the location of information is addressed. Is the information in transmission, storage, or processing? Then the security aspect is addressed. Is the issue technology, policy and procedure, or education training and awareness? Thus, one might examine the policy and procedure aspects of confidentiality of data in transmission. Or one might address the technological issues of maintaining integrity of information in storage. The McCumber cube can be seen in **FIGURE 1-4**.

No one technology is foolproof, so many security experts believe that applying multiple security services collectively that tie the transaction back to a single individual is the best way to meet business needs. The simple fact is the more evidence you gather, the harder it is for that person to deny it. Ideally, businesses want to prove it was your computer, your ID, your digital signature, and your transaction that cannot be repudiated.

What Is Governance?

Governance is both a concept and a set of specific actions an organization takes to ensure compliance with its policies, processes, standards, and guidelines. The goal is to meet business requirements; however, the focus of governance is ensuring everyone is following established rules. What is assumed in governance is that these business objectives were well understood and baked into the rules. Thus, by following the rules, you achieve these business goals. Good governance should include a good understanding of the business, so when enforcement of a rule doesn't make sense, adjustments to the governance process can take place.

Governance in the real sense is much more than a concept. An organization puts formal processes in place and creates committees to act as gateways. These are tangible acts that collectively define the governance structure of an organization. Governance is a collection of checkpoints that perform either a **quality control (QC)** or **quality assurance (QA)** function. In this context, if the governance body must approve an action, then it's a QA function. If the

governance body reviews actions after the fact, then it's a QC function. This distinction is critical in understanding how controls are managed. These terms are often misunderstood:

- Quality *assurance* functions act as a preventive control. When QA works well, it prevents mistakes from happening.
- Quality *control* functions act as a detective control. When QC works well, it improves the quality over time by affording opportunities to learn from past mistakes.

Think of this from the perspective of the forest and the trees. When you think about QA, think about looking at each tree to see if its healthy. In contrast, when you think about QC, you check to see if the forest is healthy.

Governance includes a series of oversight processes and committees. Collectively, governance ensures accountability, monitors activity, and records what is going on. What is also implied is that the governance structure will take action when the rules are ignored or not properly applied.

Why Is Governance Important?

Good governance provides assurance and confidence that rules are being followed. Who needs that assurance? First, senior management needs to know that its business objectives are being met. If the rules are being followed, there is some assurance the value promised to the business is being delivered. Also, senior management needs to know that the investment the organization has made is being properly managed. Second, regulators look at the governance structure for assurance that risks to shareholders, customers, and the public are being properly managed.

Effective governance embraces QA and QC as part of the culture. By embedding these concepts throughout, the organization promotes awareness and provides evidence of control. This is particularly important to regulators. Regulators want to see controls applied consistently. They want to know that management is aware of problems and that the company does not take shortcuts than can lead to breaking the law. Generally, the more confidence regulators have that a company has strong governance, the less regulatory oversight is used. This is especially true in highly regulated industries like healthcare and financial services. Failure to have strong governance means less opportunity to expand into new markets. Conversely, good governance means expanded business opportunities.

It's not unusual to assess the governance process of an organization. These assessments can be either self-assessments, internal audits, or regulatory reviews. For example, operational risk or compliance functions within an organization may perform a review.

The importance of governance is evident in a configuration management process. By controlling system configuration, previously mitigated vulnerabilities remain in check. This results in greater uptime rates. Change management often employs both QA and QC functions. QA governance routines review and approve each change. Whereas the QC function reviews the number of the outages caused by change and tries to improve the record, the QA function benefits from lessons learned. Governance

is important to the daily operation of an organization and should not be viewed as an occasional occurrence. Integrating the annual cost of governance into **business as usual (BAU)** budgets keeps the benefits governance provides from being viewed as an unexpected expense.

What Are Information Systems Security Policies?

Security policies are actually a collection of several documents. They generally start with a set of principles that communicate common rules across the enterprise. It is these principles that governance routines use to interpret more detailed policies. Principles are expressed in simple language. An example may be an expression of risk appetite by employing the "need-to-know" approach to the granting of access. From these security principles flow security policies that detail how the principles are put into practice.

When combined, these policy documents outline the controls, actions, and processes to be performed by an organization. An example is the requirement that a customer provide a receipt when returning an item to a retail store for a refund. That may be a simple example of a policy, but essentially, it places a control on the return process. In the same manner, ISS policies require placement of controls in processes specific to the information system. ISS policies discuss the types of controls needed but not how to build the controls. For example, a security policy may state that some data can be accessed only from the office. How the security control would be built to prevent remote access, for example, would not appear in the policy.

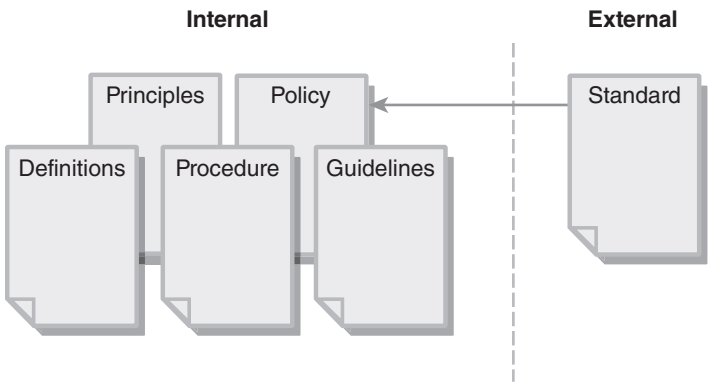
ISS policies should cover every threat to the system. They should include protecting people, information, and physical assets. Policies should also include rules of behavior such as acceptable use policies. The policies must also set rules for users, define consequences of violations, and minimize risk to the organization. Enforcement will depend on the clarity of roles and responsibilities defined in policies. Remember, you need to hold people accountable for policies. When it's unclear who is accountable, a policy becomes unenforceable. Other documents in the **policy framework** provide additional support.

There are typically six different types of documents in a framework:

- **Principles**—Establish the tone at the top and the authority by which policies are enforced
- **Policy**—A document that states how the organization is to perform and conduct business functions and transactions with a desired outcome
- **Standard**—An established industry norm or method, which can be a procedural standard or a technical standard implemented organization-wide
- **Procedure**—A written statement describing the steps required to implement a process
- **Guideline**—A parameter within which a policy, standard, or procedure is suggested but optional
- **Definitions**—Statements that define the terms used in the policy documents and set the context in which the policies documents are interpreted

Many people refer to all these documents as "security policies," but they aren't necessarily. **FIGURE 1-5** depicts the relationship among these six types of documents. The figure shows that procedures and guidelines support policies. In addition, the figure indicates that

FIGURE 1-5
Internal versus external documents.



standards influence policies. The six documents fall into two groups: internal and external. Standards are external documents. The other five are internal documents.

A **standard** can be a process or a method for implementing a solution. This involves technology, hardware, or software that has a proven record of performance. This can be a procedural or implementation standard or a technical deployment standard implemented company-wide. For the purposes of ISS, a standard is the set of criteria by which an information system must operate. Standards exert external influence on the creation of policies. An organization can have internal standards. Often these standards are tailored to the organization based on some external best practice. The proper application of standards provides assurance that lessons learned within the industry have been considered.

NOTE

Standards become the measuring stick by which an organization is evaluated for compliance. The Federal Information Processing Standards (FIPS) publications are examples of standards. You can view FIPS publications online at *https://www.nist.gov/itl/publications-0/federal-information-processing-standards-fips.*

A **policy principles document** communicates general rules that cut across the entire organization. Principles are written in plain English and focus on key risks or behaviors. When reading security principles, think of them as senior executives expressing their goals and objectives. They express core values of the organization that often include the areas where there will be zero tolerance for transgression.

A **policy** is a document that states how the organization is to perform. It describes how to conduct business functions and transactions with a desired outcome. It sets the stage for secure control of information. It is the "who does what to whom and when" document. It should reflect what leadership commitments are to protecting information. Defined roles and responsibilities lay the foundation for enforcing the policy.

NOTE

A policy is often approved by the most senior levels of management. A procedure or guideline is often approved by lower-level management responsible for the implementation of policies.

A **procedure** is a written statement describing the steps required to implement a process. Remember that procedures support policies and standards. Procedures describe how to accomplish specific tasks. A more detailed procedure produces a more error-free result. Procedures are not written just for humans to follow. Well-written procedures are often used to document requirements for automated processes.

A **guideline** sets the parameters within which a policy, standard, or procedure can be used. A guideline is optional. It is a policy-support document. Similar to procedures, guidelines help businesses operate more smoothly. They are not as rigid. Although optional, they set a direction to be taken whenever possible. Once the new approach has been widely adopted, a guideline can transition into a policy.

A **policy definitions document** is often overlooked, yet it's enormously important. It's often used by auditors and regulators when evaluating the soundness of controls. Think of it this way: If you and someone else were speaking two different languages, you might recognize some of the other person's words. Yet, the depth of the meaning of these words could easily get lost. Even common words can have many meanings in the context of a policy. For example, if a policy refers to a user ID, does the policy apply to nonhuman and human IDs equally? If the term *platform* is used, does it mean desktop or server or router? Words in policies must be rich in meaning, clear, and concise. A well-constructed policy dictionary is key to achieving this goal.

How Policies and Standards Differ

Now that you know what policies are, let's discuss the difference between policies and standards. Policies implement controls on a system to make it compliant to a standard. Standards influence the creation of policies. Standards often determine a minimum requirement but can be very detailed in nature. Laws or agreed-upon practices produce standards. Standards then become the criteria for governance or certification and accreditation.

Standards often start with industry norms. Over time, organizations that represent the industry develop and publish standards. These standards often become the measuring stick by which regulators judge organizations. It's not uncommon for a company to adjust standards to meet specific needs, and then republish them internally as a company standard or internal policy.

Be cautious when deviating too far from industry standards. There are both civil and legal penalties for not following them. Consider the Payment Card Industry Data Security Standard (PCI DSS). It calls for the following penalties:

- Fines of $500,000 per data security incident
- Fines of $50,000 per day for noncompliance with published standards

How Policies and Procedures Differ

In a similar manner, you can contrast the difference between policies and procedures. As a reminder, policies are requirements placed on processes. Procedures are the technical steps taken to achieve those policy goals. Procedures can contain step-by-step instructions on the performance of a task. They can also identify how to respond to an incident.

Within a policy framework, there could exist a policy stating the requirement for disaster recovery planning. A separate procedural document would call out specific tasks to provide recovery services. In other words, procedures are the how-to document.

Creating Policies

Clearly, policies are a key part of information systems security. Thus, creating policies is an important task that must be executed in an effective manner. In addition to the previously mentioned COBIT, other tools aid in creating policies. The International Organization for Standardization (ISO) created the standard ISO 17799, which is titled "Information Technology—Security Techniques—Code of Practice for Information Security Management." This standard establishes best practices of control objectives and controls, including security policies. This is an excellent starting point for guidance on creating information system policies.

Another source is National Institute of Standards and Technology (NIST) 800-12, titled "An Introduction to Information Security." Chapter 5 of this standard is entirely about information security policy. It provides general guidelines for developing policies. Specific policy issues such as email privacy, bring your own device (BYOD), and social media are also covered. Reviewing NIST 800-12 in conjunction with ISO 17799 will provide you with a solid understanding of policy standards.

In addition to standards such as ISO 17799 and NIST 800-12, there are several other sources for policy information. For example, the SANS organization has a number of templates you can download; these are located at *https://www.sans.org/security-resources/policies*. If you are new to developing policies, reviewing templates and the policies of other organizations is helpful.

Where Do Information Systems Security Policies Fit Within an Organization?

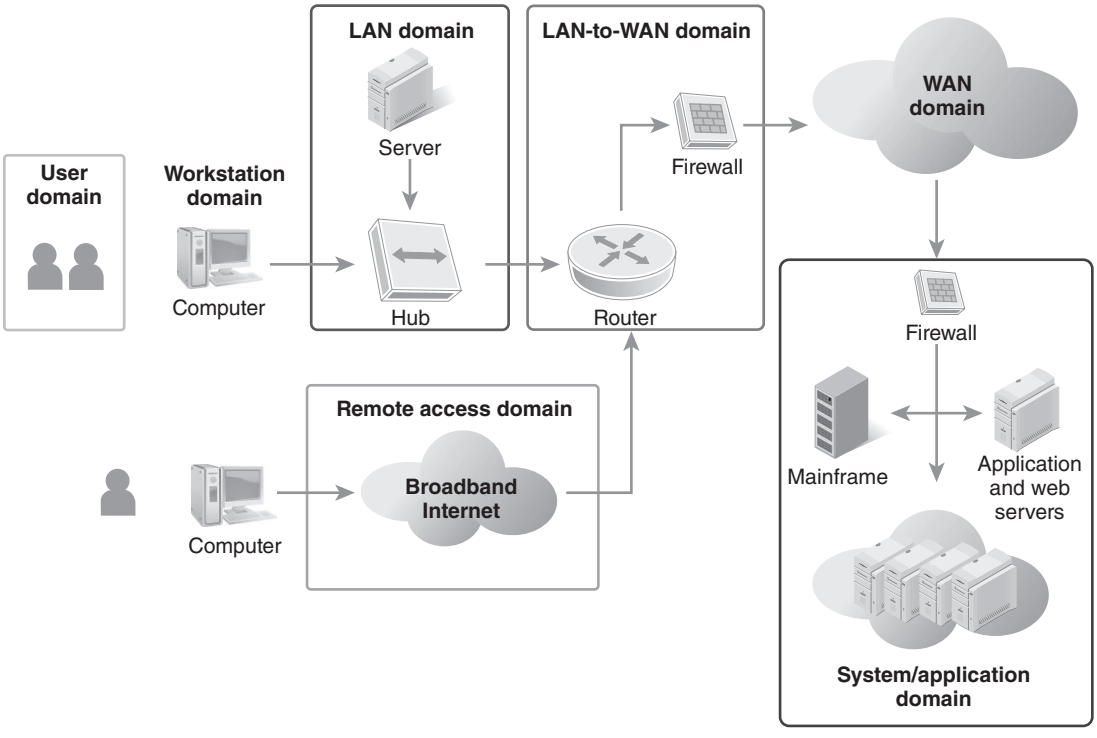
Governance over information security policies fits at more management levels. Consequently, both business and technology leaders work closely together to ensure value is delivered. However, the actual implementation of information security policies is far more complex and requires deep technical knowledge. The implementation of ISS policies often falls to the technology teams of an organization. With technology ingrained into today's society, protecting information is everyone's concern. As you discovered about information systems security, there is more to consider than just the wires and computers.

Organizations rely as much on information systems as they do on human resources. In a production facility, computers control most manufacturing devices. In a nuclear power plant, electrical generation and contamination containment rely on controlling systems to ensure the flow of power keeps the lights on safely. In a legal office, an aide researches thousands of documents and case law through a remote vast online database. These are just a few examples of the impact information systems have on a daily basis. As you can see, technology continues to become a greater part of our daily lives.

FIGURE 1-6 shows the seven domains of a typical IT infrastructure. Each domain provides unique policy requirements. Within each domain, ISS policies are vital to maintaining a secure work environment that protects the information resources critical to their individual requirements. It is becoming harder and harder to understand and protect networks when outside vendors are involved, such as a cloud service provider. You may not have direct access to vendor systems that support your network, so you may not have the assurance that your network is fully protected.

FIGURE 1-6

The seven domains of a typical IT infrastructure.



Why Information Systems Security Policies Are Important

ISS policies ensure the consistent protection of information flowing through the entire system. Information is not always static and often changes at it is processed. The information must be protected throughout the process at all times. Physical and logical access controls must work together to protect the data; however, that is not always the case. What about a disgruntled employee with elevated access privileges? How do you protect resources from someone with this kind of authorized access? Physical security has limits and should be viewed as one of several layers of control.

The following are foundational reasons for using and enforcing security policies:

- **Protecting systems from the insider threat**—The "insider threat" refers to users with authorized access. These are privileged users who would have the ability and access to wreak havoc on the system. The insider threat is probably the most significant threat to any information system. Policies help monitor authorized user activity.
- **Protecting information at rest and in transit**—Data is generally in one of two states—**data at rest**, such as on a backup tape, or **data in transit**, such as when traveling across a network. Essentially, policies help to protect data all the time.

- **Controlling change to IT infrastructure**—Change is good. Managing change is better. This reduces the risk of vulnerabilities being introduced to the system.
- **Defending the business**—Ensuring that the business can deliver reliable products and/or services will protect the company's brand.

Security polices strengthen an organization's ability to protect its information resources at all times while providing secure access to employees when they need it. Policies allow for control of the system, changes to the system, and reduction of much of the risk to the system.

Policies That Support Operational Success

The definition of operational success may vary from one organization to another. Governments may view stakeholder success differently from private industry. However, all kinds of organizations have a common concern: Is there a cost involved? Cost can be measured by either the cost of deploying policies or the cost of not having the policy in place. The cost of lacking a policy is often measured in terms of fines and legal expenses.

An effective way of expressing cost is through risk. By spending *X,* you can reduce *Y* amount of risk. For example, it would be reasonable to spend $50,000 to reduce a high risk of getting a $500,000 fine. This also allows for change in a controlled manner. It ensures that only policies that add true value are adopted. A good policy includes support for incident handling. Containing an incident can help reduce an exposure time to the organization. Identification of the reason for the incident can begin immediately and attackers potentially determined. A solution is more forthcoming, allowing the resource to be made available in a shorter amount of time. As most business folks will tell you, "Time is money."

By controlling costs and focusing on the most important risks, an organization can eliminate waste and support operational success. The key risks to the organization are reduced over time through continuous improvement achieved in part by having a good postincident handling process.

Challenges of Running a Business Without Policies

When an organization lacks policies, its operations become less predictable. Individuals will operate based on what they think is a good idea at the time. Imagine a rowing team without direction. Everyone has an oar and tries to arrive at a destination and avoid obstacles along the way. Even if you managed to arrive, think of the waste of going in circles as one side of the boat rows faster and with more urgency than the other. This assumes you can get the team to row at the same time. It's no different with policies. Policies allow an organization to row in the same direction applying the same rules, priorities, and business goals across the teams.

Here are a few challenges you can expect without policies:

- **Higher costs**—Due to wasted efforts and a lot of rework
- **Customer dissatisfaction**—Unable to produce quality because individuals make their own judgment as to what is right or good

- **Lack of regulatory compliance**—Individuals decide when and how to follow legal mandates

The result may well be legal action amounting to fines and loss of business. Depending on the industry, regulators may have the authority to close a business.

Let's look at a typical credit card breach. Assume a hacker gains access to data for 1 million credit cards. Additionally, assume the hacker accesses personal information such as Social Security numbers. Also, assume the company was out of compliance with industry norms in protecting its systems. The lack of security policies and resulting lack of methodical ways to manage risks allow vulnerabilities to these systems to go undetected. This could lead to lawsuits by customers and shareholders.

Dangers of Not Implementing Policies

If security policies are to ensure information is properly protected, failing to implement policies leaves information vulnerable. The information may be vulnerable to an attack or mishandling. Some employers say, "Our employees are the smartest in their fields," or, "We've been operating like that for years without a single problem (knock on wood)." These are also responses to the question, "Why implement policies?"

The dangers of not implementing policies are unexpected and undesirable outcomes. In the event of an ISS incident, employees will not know what to do, how to react, or whom to notify. This will lead to general confusion. As they're trying to figure out the answers to those questions, an attacker may be copying more information from the system.

Good security policies include creating awareness of security's benefits. This includes benefits to the employee. When good policies are implemented, they protect both customer and employee. With good policies in place, even if there is a data breach, the damage may be limited.

Dangers of Implementing the Wrong Policies

Similar to not implementing policies is implementing the wrong policies. You should create policies to address the proper processes, or detrimental consequences can occur. For example, consider a policy that states all employees should be granted administrator privileges to a system. Under this policy, the basic tenets of information assurance cannot be guaranteed. Users will have access to all information, which is probably not intended, nor is it a best security practice. Security policy is often a family of policies, so be sure they do not conflict with one another. In the event of a data breach, all employees with access immediately become suspect. This can often delay investigations.

When Do You Need Information Systems Security Policies?

"Timing is everything." This is most likely the No. 1 tenet of comedians. The same applies to the timeliness of policies. Why implement a policy on milking cows when your business model raises chickens? The possibility exists that your farm will expand operations one day, but there is no reason to write policies until that expansion occurs.

There will be times when the need for an ISS policy is evident. There is always a need for foundational security policies. This includes defining basic data handling and acceptable use policies. Security policies need to ensure that new technology is not introduced without a supporting set of policies in place. Another consideration is that you may have a process that occurs daily and all the involved employees are aware of that process. The employees may modify the process. But without configuration management control, modifications can make secure systems nonsecure. Or an important process may be undocumented, even though employees know all the steps. This is the perfect opportunity to formalize a written procedure.

Business Process Reengineering (BPR)

Business processes are constantly under scrutiny for improvement. As that business process life cycle is accomplished, the process is improved and changed; however, the associated policies must also be changed and updated. Typically, the associated policies and procedures recognized during the life cycle are operational in nature. Policies that support operations, like security policies, are not always considered. Failing to update those policies and procedures leaves a window of opportunity for error or disaster.

The process change could be dramatic enough to introduce new security vulnerabilities. If the equipment operating within the process completely changes, old security vulnerabilities reappear. Therefore, it is imperative to ensure that when reengineering any business process, you also review security. This will ensure that **business process reengineering (BPR)** includes ISS concerns, and those policies and procedures are updated as needed.

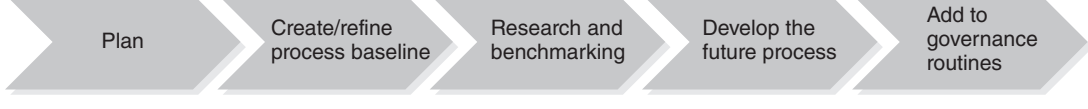
FIGURE 1-7 shows the four phases of BPR. Phase 1 is the planning phase. Phase 2 sees the creation or modification of the process baseline. Research and benchmarking happen in Phase 3. Phase 4 develops the future process; it is during this phase that new policies are written or current ones are updated.

Continuous Improvement

You can view **continuous improvement** as finding a better way or as a lesson learned. As employees find new ways to improve a system or process, you need to have a way to capture their ideas. The concept of continuous improvement applies to all aspects of ISS and IA. For example, when looking at availability issues, you may come across an authentication weakness. Regardless of how the weakness or risk was found, you need to capture the

FIGURE 1-7

Basic business process reengineering.



information, assess the importance, and apply an improvement. Often, lessons learned flow from effective governance. Quality control will reflect what worked well and what didn't. The part that didn't work well represents the lessons learned. Sometimes this means changing policy. When policy goals cannot be achieved, enforcement becomes impossible, and the overall security policy framework is weakened.

The driver for "finding a better way" should not be a system crash or breach. In those cases, you may have to deal with lessons learned from the incident. Think of continuous improvement as a suggestion box. Employees identify needed changes and write a suggestion. The suggestion is either accepted or rejected. If accepted, it enters the formal reengineering process.

Making Changes in Response to Problems

Even with a sound policy framework, issues will occur. Depending on the criticality of the issue, policy implementation or change can occur at any time in the process. Policy changes brought about in this manner help avoid future incidents. In a perfect environment, policies fall into place before incidents occur; however, most organizations do not operate in a perfect environment. Once an event not covered by a policy occurs, an event analysis takes place, and a recommendation is drafted. For events that are noncritical in nature, policy drafting comes about in concert with the remediation process. If it is more critical in nature, remediation should occur prior to writing the policy.

Why Enforcing and Winning Acceptance for Policies Is Challenging

There are many barriers to policy acceptance and enforcement. Without acceptance and enforcement of policies, employees could operate in a laissez-faire state. This runs counter to the business goals. It will inevitably lead to an employee not taking policy seriously. Employees taking shortcuts or ignoring policy can have serious impacts. Within an organization, there must be support at all levels, from the top to the bottom. Employees must have a stake in ISS. They must understand how those policies and procedures affect them and their business area. If they have a stake in creating or approving policies, they will be more likely to accept those policies. The following is a list of policy acceptance challenges:

- **Organizational support at all levels**—Without cohesive support from all levels of the organization, acceptance and enforcement will fail.
- **Giving employees a stake**—There must be something to motivate employees to buy in to the process. This could be some kind of award for participating, or disciplinary action if they don't.
- **Policy awareness and understanding**—Employees must know a policy exists and understand what it means. Crafting the document to make this easy can be challenging.

NOTE

The biggest hindrance to implementation of policies is the human factor. Human beings must first fully understand the policy. Then the policy must be implemented and adhered to. Both of these activities can fail due to human error.

- **Rewarding and recognizing behavior**—Employees must see good examples to model their behavior after.
- **Hold individuals accountable**—Employees must know there is a consequence for repeated noncompliance.

Enforcement of policies can be just as difficult as policy acceptance. There are several reasons why enforcement is challenging. The language in which policies are written can be vague enough to be unenforceable. Infractions are not reported, which is often a key contributor to the lack of enforcement. Other business areas in the organization, such as human resources or the legal department, might not be part of the enforcement process. This can give employees license to either disregard the policies or perform actions contrary to them. The following list recaps policy enforcement challenges:

- Poorly written policies
- Failure to report infractions
- Lack of involvement in enforcement of key departments and management
- Lack of clearly defined roles and responsibilities

CHAPTER SUMMARY

This chapter defined foundational ISS concepts and key terms. You learned about the key tenets of ISS management to ensure confidentiality, integrity, availability, authentication, and nonrepudiation. Additionally, you read that information systems security (ISS) and information assurance (IA) are two separate but similar concepts. Associated with IA and ISS is governance. Governance ensures people are following the rules, such as policies, regulations, standards, and procedures. You also read about the importance of quality control and quality assurance.

There are several situations when security policies are to be considered. Opportunities include:

- New business processes
- Changes in current business processes
- Business process reengineering (BPR)
- Incident occurrence

You read about where policies fit within an organization to meet operational and governance requirements. These include all seven domains, across the business spectrum. ISS policies are important for several reasons. A primary reason is controlling authorized access to information. Another reason is to control change to systems. You read about how to express risk in terms of threats and vulnerabilities. Finally, you learned about policy acceptance and enforcement, and factors that make those processes difficult. Employee support is required at all levels for policy buy-in and enforcement. Enforcement also hinges on effective policy writing.