CHAPTER 3

What Is the Scope of an IT Compliance Audit?

AUDITS 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.

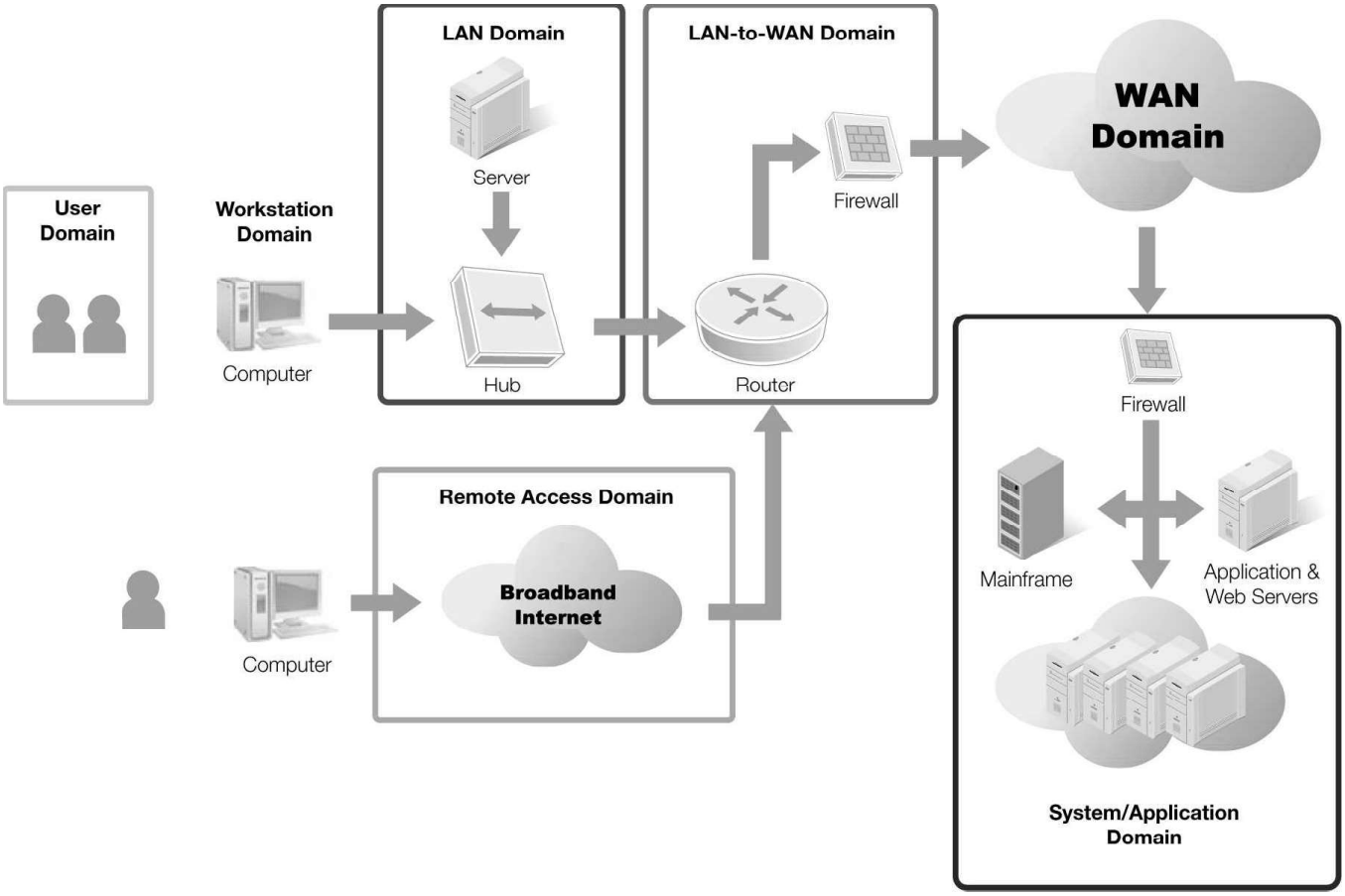

FIGURE 3-1 The seven domains of a typical IT infrastructure.

- **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 at 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.

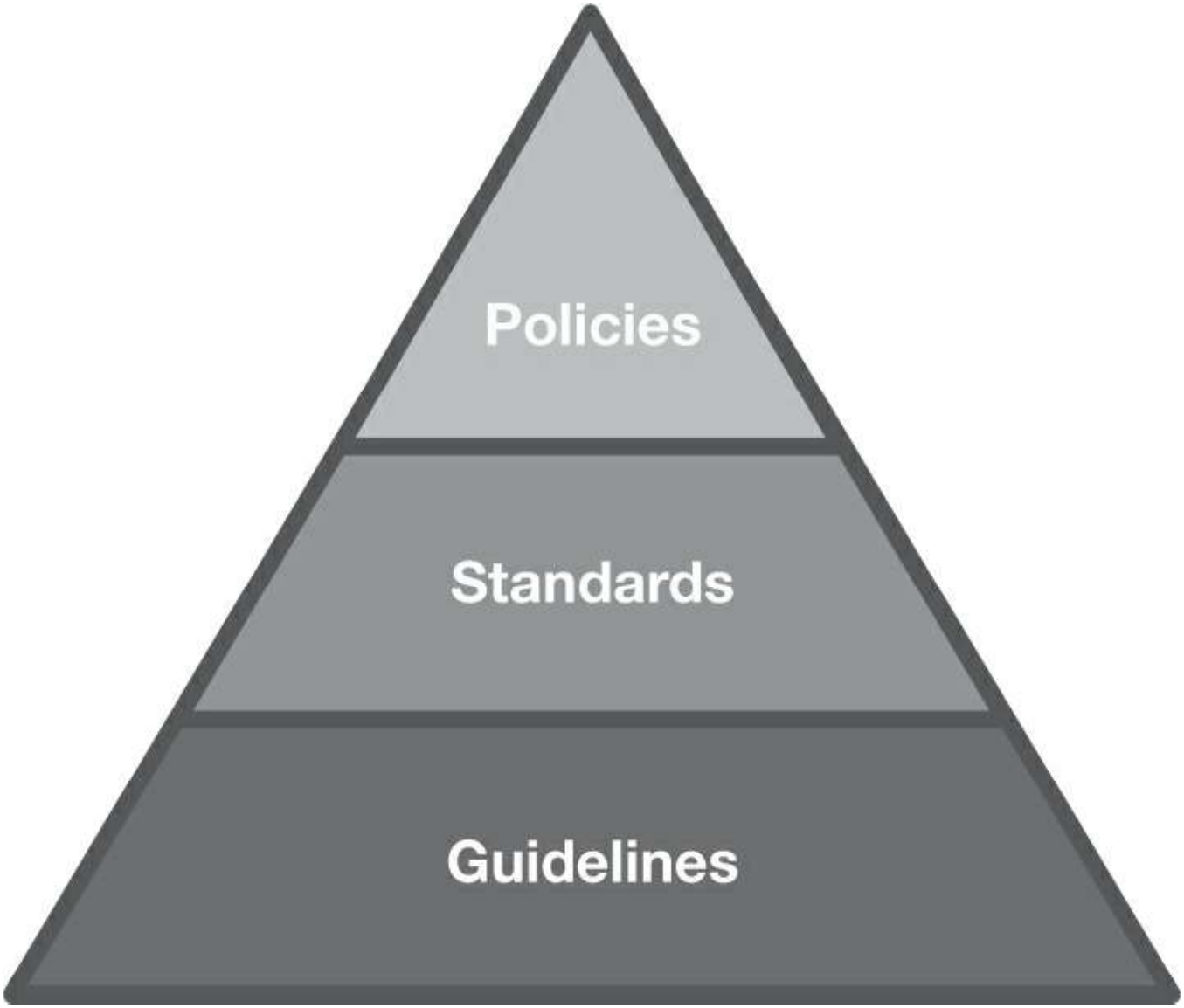

FIGURE 3-2 A policy framework.

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