Chapter 5. Planning an IT Infrastructure Audit for Compliance

AUDIT PLANNING SHOULD NOT BE OVERLOOKED. What goes into the planning process directly affects the quality of the outcome. The planning stage is the first step and takes place before any of the detailed audit work begins. A proper plan ensures that resources are focused on the right areas and that potential problems are identified early. A successful audit first outlines what's supposed to be achieved as well as what procedures will be followed and the required resources to carry out the procedures.

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

Chapter 5 Topics

This chapter covers the following topics and concepts:

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

Chapter 5 Goals

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

- Understand how to define the scope and frequency of an audit
- Identify the key requirements for an audit
- Understand the importance of risk management in assessing security controls

- Understand information and resources needed for an IT audit
- Relate the IT security policy framework into the seven domains of IT infrastructure
- Understand why monitoring requirements help with an IT audit
- Identify security control points
- Differentiate between the project management tasks of an IT audit

Defining Scope, Goals and Objectives, and Frequency

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

Prior to performing an audit, the auditor should first define the audit scope. The scope includes the area or areas to be reviewed as well as the time period. Experienced auditors know it's just as important to define what will be audited as it is to define what will not be audited. If scope is not clearly defined, scope creep occurs, likely increasing the auditor's workload.

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

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

- Data
- Applications systems
- Technology
- Facilities
- Personnel

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

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

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

Project Management

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

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

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

Identifying Critical Requirements for the Audit

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

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

Implementing Security Controls

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

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

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

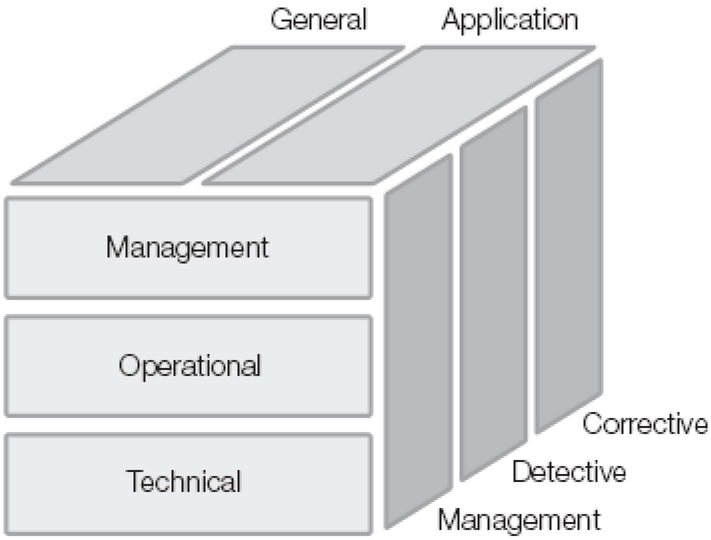

Figure 5-1. Control classifications.

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

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

- **Technical controls**—Includes controls that are performed by the IT systems. Examples include:
  - Identification and authorization
  - Logical access control
  - Audit trails
  - Cryptography

Controls are further classified as being preventive, detective, or corrective. Preventive controls stop a particular threat in the first place. A door lock on a home is a simple example of a preventive control. A detective control identifies that a threat is present. A home alarm system, for example, is a common detective control. Some people even advertise they have an alarm system by putting a notice on the door or a sign in the yard. In this case, this also serves as a preventive control. Finally, a reactive or corrective control can lessen the effects of a threat. The home alarm system that also notifies the police department is an example of a reactive control. Antivirus software is a common control that spans all three. It can prevent a system from getting a virus in the first place. It can detect if a virus is on the system. Finally, it can react and correct the situation by removing or quarantining the virus.

Protecting Privacy Data

Audits of IT infrastructure around security are common. However, due to recent legislation regarding the need to protect personally identifiable information, audits specific to privacy are more commonplace than before. ISACA defines privacy within the context of information systems as "adherence to trust and obligation in relation to any information relating to an identified or identifiable individual (data subject). Management is responsible to comply with privacy in accordance with its privacy policy or applicable privacy laws and regulations."[1]

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

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

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

A privacy audit should consider what privacy laws apply to the organization. Auditors should consider who has responsibility for privacy within the organization. This includes the roles of legal counsel and if a **chief privacy officer (CPO)** role is established. Finally, the policies and procedures specific to privacy should be examined.

Assessing IT Security

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

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

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

Table 5-1. The Generally Accepted Privacy Principles.[2]

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

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

Risk Management

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

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

An example of an IT risk framework compatible with ERM is ISACA's Risk IT. The Risk IT framework is based on and complements Control Objectives for Information and related Technology (COBIT). Risk IT provides a comprehensive framework for not just assessing risk, but also guidance around governance and response. Whereas COBIT provides a framework of controls to minimize risk, Risk IT provides the framework for managing risk. Another example of an information security risk management framework is ISO standard **ISO/IEC 27005.** In addition to providing guidelines for information security risk management, this ISO standard also supports the concepts within ISO/IEC 27001.

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

There are several methodologies for assessing risk specific to IT environments. **NIST 800-30**, "Risk Management Guide for Information

Technology Systems," is one such example. This guide provides a practical nine-step process, as follows:

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

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

Threat Analysis

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

NOTE

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

Threats can be grouped through a combination of the following:

- External or internal
- Natural or man-made
- Intentional or accidental

Table 5-2. Example of threats, motivations, and threat actions.

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

Information about threats such as natural disasters will be readily available and easily obtained by private and governmental resources. The threats that are more difficult to identify are those that pertain specifically to the organization. Table 5-2 provides a summary of man-made threats identified in NIST 800-30. The table includes a list of threats, motivations, and methods that might be used to carry out an attack. The methods are also known as **threat actions.**

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

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

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

Vulnerability Analysis

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

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

TIP

The MITRE Corporation catalogs vulnerabilities in the Common Vulnerabilities and Exposures (CVE), which includes over 40,000 items.

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

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

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

Risk Assessment Analysis—Defining an Acceptable Security Baseline Definition

Given the previous inputs, the final step is to determine the level of risk. When pairing threats and vulnerabilities, risk is determined primarily by three functions: 1) the likelihood of a threat to exploit a given vulnerability; 2) the impact on the organization if that threat against the vulnerability is achieved; and 3) the sufficiency of controls to either eliminate or reduce the risk. At this point, matrixes and other mechanisms are useful for quantitatively understanding risk. Such matrixes typically categorize the impact and the likelihood of threats as either being low, medium, or high. The product of this results in a risk being low, medium, or high.

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

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

NOTE

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

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

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

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

Obtaining Information, Documentation, and Resources

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

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

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

Aside from just understanding what regulatory and industry requirements the organization must adhere to, auditors should have a much larger understanding of the business. General knowledge about the business can be gained by gathering information on business and reporting cycles, key business processes, and key personnel to interview. Strategic objectives of an organization reveal details about the organization in the future and how this will affect their information systems. In addition, information about the operational objectives for internal control provides relevant information to the current state of the organization.

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

NOTE

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

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

- Administrative documentation
- System documentation

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

Existing IT Security Policy Framework Definition

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

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

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

NOTE

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

Finally, always remember that policies are fundamental to the organization's actions. The policies drive the behavior of the people within an organization and even the technologies acquired. One of executive management's responsibilities is to set goals. Management further supports these goals with a set of objectives.

These objectives are communicated throughout the organization by policies. This applies not just to IT security policies, but also to policies across the organization. The policies set the standards, which help drive the business to achieve its goals. As a result, an organization's policies are quite important if they are expected to drive actions and behaviors from the top down. Therefore, high-level policies should be approved and signed by executive management.

TIP

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

Configuration Documentation for IT Infrastructure

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

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

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

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

- Firewalls
- Web servers
- Mail servers
- Domain Name System (DNS) servers
- File Transfer Protocol (FTP) servers

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

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

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

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

- Lack of controls
- Override of controls
- Fraudulent activity

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

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

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

The next two steps constitute the actual interview. The opening sets the tone for the remainder of the interview. Opening with a positive tone and clear expectations, combined with thorough preparation in step one, makes conducting the interview much easier. This leads us into the next step, which is asking the questions. At this point, however, it is not enough to have just well-thought-out questions. The auditor must be adept at listening as well. The auditor should understand lines of management and how they might influence the interviewee's responses. Closing the interview occurs after the auditor has asked all the required questions, or once time is up. The interview should ideally end politely and on an upbeat note. The auditor should thank the interviewee for his or her time, and suggest an agreed-upon protocol, should the auditor require anything else. This leads into the final step of recording. Taking notes is certainly acceptable during the interview process, but it can be disruptive to the interview flow. Even if notes are taken, after the interview, the auditor should immediately review the notes and organize them as needed.

NIST Standards and Methodologies

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

The Computer Security Division (CSD) of NIST provides these popular publications along with many more. All of their publications are a result of their research on IT security issues. The publications they provide include:

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

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

- SP 800-50, "Building an Information Technology Security Awareness and Training Program"
- SP 800-57, "Recommendation for Key Management"
- SP 800-58, "Security Considerations for Voice Over IP Systems"
- SP 800-61, "Computer Security Incident Handling Guide"
- SP 800-68, "Guide to Securing Microsoft Windows XP Systems for IT Professionals"
- SP 800-95, "Guide to Secure Web Services"
- SP 800-115, "Technical Guide to Information Security Testing and Assessment"
- SP 800-123, "Guide to General Server Security"
- SP 800-70, "National Checklist Program for IT Products—Guidelines for Checklist Users and Developers"

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

Organizing the IT Security Policy Framework Definitions for the Seven Domains of a Typical IT Infrastructure

The IT security policy framework includes policies, standards, and guidelines. Each of these includes technology, processes, and personnel. The seven domains of typical IT infrastructure need to be mapped into the framework. As a refresher from Chapter 3, the seven domains of typical IT infrastructure are as follows:

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

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

technical TIP

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

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

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

Identifying and Testing Monitoring Requirements

Perhaps one of the most important and beneficial elements of an IT security program for auditors is monitoring. All frameworks include a control objective for regularly assessing and monitoring IT systems and controls. For example, COBIT has an entire domain defined for monitoring and evaluating internal controls. COBIT states this domain helps provide answers to the following questions:

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

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

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

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

- Monitor and Evaluate IT Performance
- Monitor and Evaluate Internal Control
- Ensure Compliance with External Requirements
- Provide IT Governance

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

Identifying Critical Security Control Points That Must Be Verified Throughout the IT Infrastructure

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

A great example is the **Consensus Audit Guidelines (CAG)** published by SANS in 2009. This guideline is also known as the SANS Top 20 Critical Security Controls. This includes 20 technical control areas deemed critical, which were introduced in Chapter 3. These 20 controls, although not prioritized in any order, do establish an overall prioritized baseline of security measures and controls that should be in place at most organizations. Of the 20 controls, 15 can in part or whole be monitored through automated means. As a result, this provides not only a baseline from which to identify security controls, but also a way to verify them efficiently and continuously.

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

TIP

The Consensus Audit Guidelines provide an appendix that maps the top 20 critical security controls to specific controls within NIST SP 800-53.

Building a Project Plan Organizing the IT Infrastructure Audit Approach, Tasks, Deliverables, Timelines, and Resources Needed

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

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

- **Electronic work papers**—Provides a document management system to help centralize and provide workflow management of the audit process.
- **Project management software**—Includes mechanisms for managing any project, including auditing projects. These software packages help track progress to established milestones. Project management software is helpful in defining the timeline of the plan and for reporting upon status.
- **Flowcharting software**—Provides a way to visually document processes.

> **FYI**
>
> Although resources and budgets can be tight, organizations need to ensure adequate auditing resources. The Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2 states that "an ineffective control environment was a significant deficiency and a strong indicator that a material weakness exists."[3]

- **Open issue tracking software**—Allows for easy tracking of audit deficiencies and areas that still need to be addressed. In many cases, this function can be integrated or included within a document management system.
- **Audit department Web site**—Internal auditing departments typically have an intranet-based solution that provides for collaboration and communication. Even external auditors benefit from maintaining secured Internet-based portals that provide the same functions.

The previous list of tools is useful for the overall management of the audit. During the course of an audit, however, auditors will likely use additional tools to help with the efficiency and effectiveness of carrying out the audit. Various programs and utilities exist that can help automate tests during the course of the audit. In the next chapter on conducting an audit, you will learn about the many options available. Meanwhile, from a planning perspective, it's important to understand that identification of such tools should be included as part of the planning process.

CHAPTER SUMMARY

An audit plan is a necessary step prior to conducting the actual audit and reporting findings. Identifying and prioritizing risks is a key component of the audit plan. This provides the necessary information to make informed decisions about the scope and objectives of an audit and what resources will be required. Performing key tasks such as aligning the scope with the objectives and gathering all pertinent information beforehand makes the process of testing controls much easier.

The next two chapters look at conducting an audit of IT infrastructure for compliance and the subsequent audit report. Conducting the audit and reporting upon the results will be a direct reflection upon the approved plan.

KEY CONCEPTS AND TERMS

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

CHAPTER 5 ASSESSMENT

1. Which one of the following can an audit help identify?
    1. Fraud
    2. Ineffective IT practices

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

    4. Technical controls

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

ENDNOTES

1.

ISACA, `http://www.isaca.org/Template.cfm?Section=Standards&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18719`(accessed March 22, 2010).

2.

AICPA, `http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/Introducing+Generally+Accepted+Privacy+Principles.htm`(accessed March 22, 2010).

3. Public Company Accounting Oversight Board (PCAOB) Auditing Standard No.
2, `http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_2_Appendix_E.aspx`(accessed March 22, 2010).