CHAPTER 5

**Planning an IT Infrastructure Audit for Compliance**

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

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

**Chapter 5 Topics**

This chapter covers the following topics and concepts:

•  How to define the scope, objectives, goals, and frequency of an audit

•  What the critical requirements for an audit are

•  How to assess IT security

•  How to obtain information, documentation, and resources

•  How to map the security policy framework definitions to the seven domains of IT infrastructure

•  How to identify and test monitoring requirements

•  How to identify critical security control points that must be verified throughout the IT infrastructure

•  How to build a project plan

**Chapter 5 Goals**

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

•  Define the scope and frequency of an audit

•  Identify the key requirements for an audit

•  Understand the importance of risk management in assessing security controls

•  Identify the information and resources needed for an IT audit

•  Relate the IT security policy framework to the seven domains of IT infrastructure

•  Understand why monitoring requirements help with an IT audit

•  Identify security control points

•  Differentiate between the project management tasks of an IT audit

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

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

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

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

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

•  Data

•  Applications

•  Technology

•  Facilities

•  Personnel

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

•  Not providing enough resources

•  Limiting the time frame

•  Preventing the discovery of audit evidence

•  Restricting audit procedures

•  Withholding relevant historical records or information about past incidents

**Project Management**

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

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

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

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

**Identifying Critical Requirements for the Audit**

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

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

Implementing Security Controls

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

Controls can be classified into different groups to aid in understanding how they fit into the overall security of a system. [Figure 5-1](http://e.pub/ftu7d5ig0nyyjml5juao.vbk/OEBPS/xhtml/14_Chapter05.xhtml#fig5_1) illustrates the different dimensions of control classifications. Understanding the classifications provides auditors with a foundation to identify and assess critical controls.

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

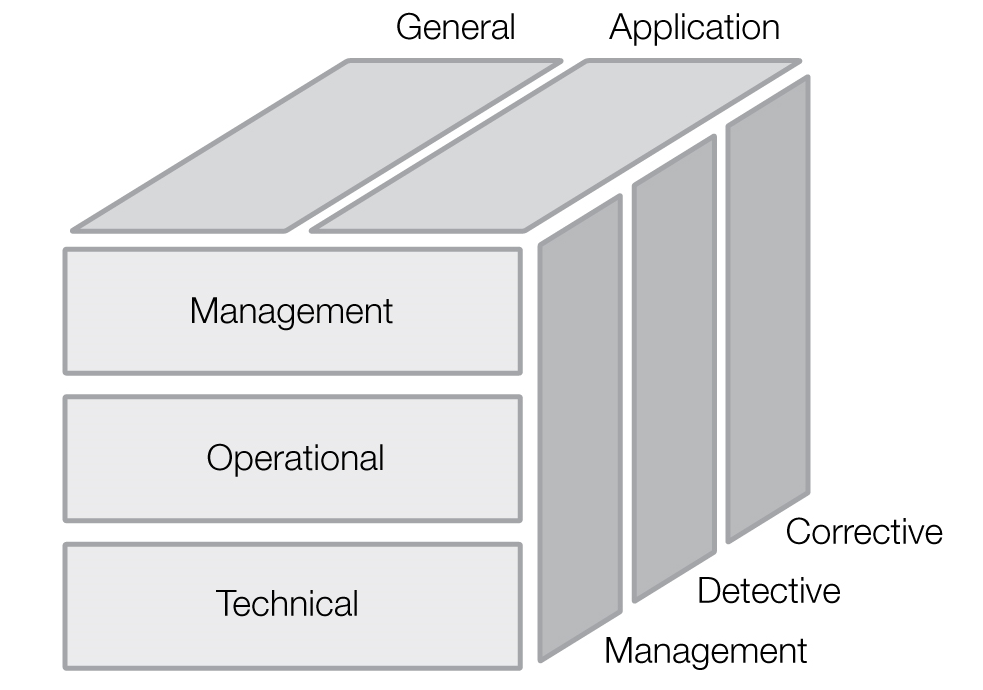


FIGURE 5-1 Control classifications.

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

•  Management controls—These include controls typically governed by management as part of the overall security program. Examples include the following:

•  Security policy

•  Security program management

•  Risk management

•  Security and planning in the system development life cycle

•  Assurance

•  Operational controls—These include controls that are implemented by people rather than systems. These controls are often interrelated with both management and technical controls. Examples include the following:

•  Personnel and user issues

•  Contingency and disaster planning

•  Incident response and handling

•  Awareness, training, and education

•  Computer support and operations

•  Physical and environmental security

•  Technical controls—These include controls that are performed by the IT systems. Examples include the following:

•  Identification and authorization

•  Logical access control

•  Audit trails

•  Cryptography

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

**NOTE**

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

Protecting Privacy Data

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

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

•  What type of personal information is processed and stored?

•  Where is it stored?

•  How is it managed?

[Table 5-1](http://e.pub/ftu7d5ig0nyyjml5juao.vbk/OEBPS/xhtml/14_Chapter05.xhtml#tab5_1) outlines guidance for privacy audits established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). This guidance is named **Generally Accepted Privacy Principles (GAPP)**.

A privacy audit should consider what privacy laws apply to the organization. Auditors should consider who has responsibility for privacy within the organization. This includes the roles of legal counsel and whether a **chief privacy officer (CPO)** role is established. (The CPO is a senior-level position responsible for the overall management of an organization’s privacy program.) Finally, the policies and procedures specific to privacy should be examined.

TABLE 5-1 The Generally Accepted Privacy Principles.

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

**Assessing IT Security**

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

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

•  Is a control even required?

•  How much effort or money should be spent on a control?

•  Is the control effective?

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

Risk Management

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

•  Aligning risk appetite and strategy—This helps the organization to manage the uncertainty with consideration of the goals of the organization.

•  Enhancing risk response decisions—This improves the organization’s ability to make decisions about how to better manage risk.

•  Reducing operational surprises and losses—This enhances the organization’s ability to identify potential events or threats and react appropriately.

•  Identifying and managing multiple and cross-enterprise risks—This helps the organization to consider related risks from across the organization and provides a unified response across the varying risks.

•  Seizing opportunities—This helps the organization to recognize events from which new opportunities can be pursued.

•  Improving deployment of capital—This improves how organizations divide their financial resources to enhance performance and profitability.

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

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

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

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

•  Threat identification—Identify potential methods or situations that could exploit a weakness.

•  Vulnerability identification—Identify flaws or weaknesses that can be triggered or exploited, which might result in a breach.

•  Control analysis—Analyze controls to reduce the likelihood of a threat successfully exploiting a vulnerability.

•  Likelihood determination—Determine the likelihood of an attack by considering the motivation and capability of the threat source along with the nature of the vulnerability in relation to the current controls.

•  Impact analysis—Determine the impact of a successful attack on a vulnerability by a threat. Consider the mission of a system, data criticality, and data sensitivity.

•  Risk determination—Consider the likelihood, magnitude of impact, and adequacy of controls as an equation of risk.

•  Control recommendations—Consider controls to reduce the level of risk to an acceptable level.

•  Results documentation—Document for management the observations on threats and vulnerabilities as well as risks overall and recommended controls.

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

**NOTE**

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

Threat Analysis

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

Threats can be grouped as a combination of the following:

•  Adversarial

•  Accidental

•  Structural

•  Environmental

Information about threats such as natural disasters is readily available and easily obtained through private and governmental resources. The threats that are more difficult to identify are those that pertain specifically to the organization. [Table 5-2](http://e.pub/ftu7d5ig0nyyjml5juao.vbk/OEBPS/xhtml/14_Chapter05.xhtml#tab5_2) provides examples of various adversarial threat sources. The table includes a list of threats, motivations, and methods that might be used to carry out an attack. The methods are also known as **threat actions**.

All the threats in [Table 5-2](http://e.pub/ftu7d5ig0nyyjml5juao.vbk/OEBPS/xhtml/14_Chapter05.xhtml#tab5_2) represent varying degrees of potential risks if they are accompanied by vulnerabilities. Each organization will identify its unique threats. Even businesses with multiple locations will have threats specific to that location. To really understand threats, think about your own personal situation. What threats are common to you and where you live? Do these threats change as you travel? What threats exist based on your lifestyle and goals?

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

•  Low—No previous history of the threat, and the threat is not likely to occur

•  Medium—Some history of the threat, and the threat might occur

•  High—Substantial history of the threat, and the threat is likely to occur

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

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

Vulnerability Analysis

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

•  Vulnerability lists and databases published by industry organizations

•  Security advisories

•  Software and security analysis using automated tools

**TIP**

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

It is important to consider threats relative to vulnerabilities. Think about operating system patches issued by Microsoft or Apple. Typically, these fix potential vulnerabilities, which were previously unknown and have since been discovered. In most cases, these vulnerabilities affect a particular piece of the system. Say, for example, Microsoft issues a patch to fix a vulnerability for a particular service of the operating system. However, what if you don’t use this service or the service is turned off? In this case, the vulnerability is not really vulnerable. What if the particular system you use does not and will never be connected to the Internet? In this case, the threat in question does not exist. This is why

(Martin 100-111)

Martin, Weiss,, Solomon, G.. *Auditing IT Infrastructures for Compliance, 2nd Edition*. Jones & Bartlett Learning, 07/2015. VitalBook file.

The citation provided is a guideline. Please check each citation for accuracy before use.