PART THREE: Management Issues

CHAPTER 14

IT Security Management and Risk Assessment

LEARNING OBJECTIVES

After studying this chapter, you should be able to:

- Understand the process involved in IT security management.
- Describe an organization's IT security objectives, strategies, and policies.
- Detail some alternative approaches to IT security risk assessment.
- Detail steps required in a formal IT security risk assessment.
- Characterize identified threats and consequences to determine risk.
- Detail risk treatment alternatives.

In previous chapters, we discussed a range of technical and administrative measures that can be used to manage and improve the security of computer systems and networks. In this chapter and the next, we will look at the process of how to best select and implement these measures to effectively address an organization's security requirements. As we noted in Chapter 1, this involves examining three fundamental questions:

1. What assets do we need to protect?
2. How are those assets threatened?
3. What can we do to counter those threats?

IT security management is the formal process of answering these questions, ensuring that critical assets are sufficiently protected in a cost-effective manner. More specifically, IT security management consists of first determining a clear view of an organization's IT security objectives and general risk profile. Next, an IT security **risk assessment** is needed for each asset in the organization that requires protection; this assessment must answer the three key questions listed above. It provides the information necessary to decide what management, operational, and technical controls are needed to either reduce the risks identified to an acceptable level or otherwise accept the resultant risk. This chapter will consider each of these items. The process continues by selecting suitable controls then writing plans and procedures to ensure these necessary controls are implemented effectively. That implementation must be monitored to determine if the security objectives are met. The whole process must be iterated, and the plans and procedures kept up-to-date, because of the rapid rate of change in both the technology and the risk environment. We will discuss the latter part of this process in Chapter 15. The following chapters, then, will address specific control areas relating to physical security in Chapter 16, human factors in Chapter 17, and auditing in Chapter 18.

14.1 IT SECURITY MANAGEMENT

The discipline of IT security management has evolved considerably over the last few decades. This has occurred in response to the rapid growth of, and dependence on, networked computer systems, and the associated rise in risks to these systems. In the last decade, a number of national and international standards have been published. These represent a consensus on the *best practice* in the field. The International

Table 14.1 ISO/IEC 27000 Series of Standards on IT Security Techniques

27000:2016	"Information security management systems—Overview and vocabulary" provides an overview of information security management systems, and defines the vocabulary and definitions used in the 27000 family of standards.
27001:2013	"Information security management systems—Requirements" specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System.
27002:2013	"Code of practice for information security management" provides guidelines for information security management in an organization and contains a list of best-practice security controls. It was formerly known as ISO17799.
27003:2010	"Information security management system implementation guidance" details the process from inception to the production of implementation plans of an Information Security Management System specification and design.
27004:2009	"Information security management—Measurement" provides guidance to help organizations measure and report on the effectiveness of their Information Security Management System processes and controls.
27005:2011	"Information security risk management" provides guidelines on the information security risk management process. It supersedes ISO13335-3/4.
27006:2015	"Requirements for bodies providing audit and certification of information security management systems" specifies requirements and provides guidance for these bodies.

Standards Organization (ISO) has revised and consolidated a number of these standards into the ISO 27000 series. Table 14.1 details a number of recently adopted standards within this family. In the United States, NIST has also produced a number of relevant standards, including NIST SP 800-18 (*Guide for Developing Security Plans for Federal Information Systems*, February 2006), NIST SP 800-30 (*Guide for Conducting Risk Assessments*, September 2012), and NIST SP 800-53 (*Security and Privacy Controls for Federal Information Systems and Organizations*, January 2015). NIST also released the "*Framework for Improving Critical Infrastructure Cybersecurity*" in 2014, to provide guidance to organizations on systematically managing cybersecurity risks. With the growth of concerns about corporate governance following events such as the global financial crisis and repeated incidences of the loss of personal information by government organizations and other businesses, auditors for such organizations increasingly require adherence to formal standards such as these.

For our purposes, we can define **IT security management** as follows:

IT SECURITY MANAGEMENT: The formal process used to develop and maintain appropriate levels of computer security for an organization's assets, by preserving their confidentiality, integrity, availability, accountability, authenticity, and reliability. The steps in the IT security management process include:

- determining the organization's IT security objectives, strategies, and policies.
- performing an IT security risk assessment that analyzes security threats to IT assets within the organization, and determines the resulting risks.
- selecting suitable controls to cost effectively protect the organization's IT assets.

- writing plans and procedures to effectively implement the selected controls.
- implementing the selected controls, including provision of a security awareness and training program.
- monitoring the operation, and maintaining the effectiveness, of the selected controls.
- detecting and reacting to incidents.

This process is illustrated in Figure 14.1 (adapted from figure 1 in ISO 27005 (*Information security risk management*, 2011) and figure 1 in part 3 of ISO 13335 (Management of information and communications technology security, 2004)), with a particular focus on the internal details relating to the **risk assessment** process. IT security management needs to be a key part of an organization's overall management plan. Similarly, the IT security risk assessment process should be incorporated into the wider risk

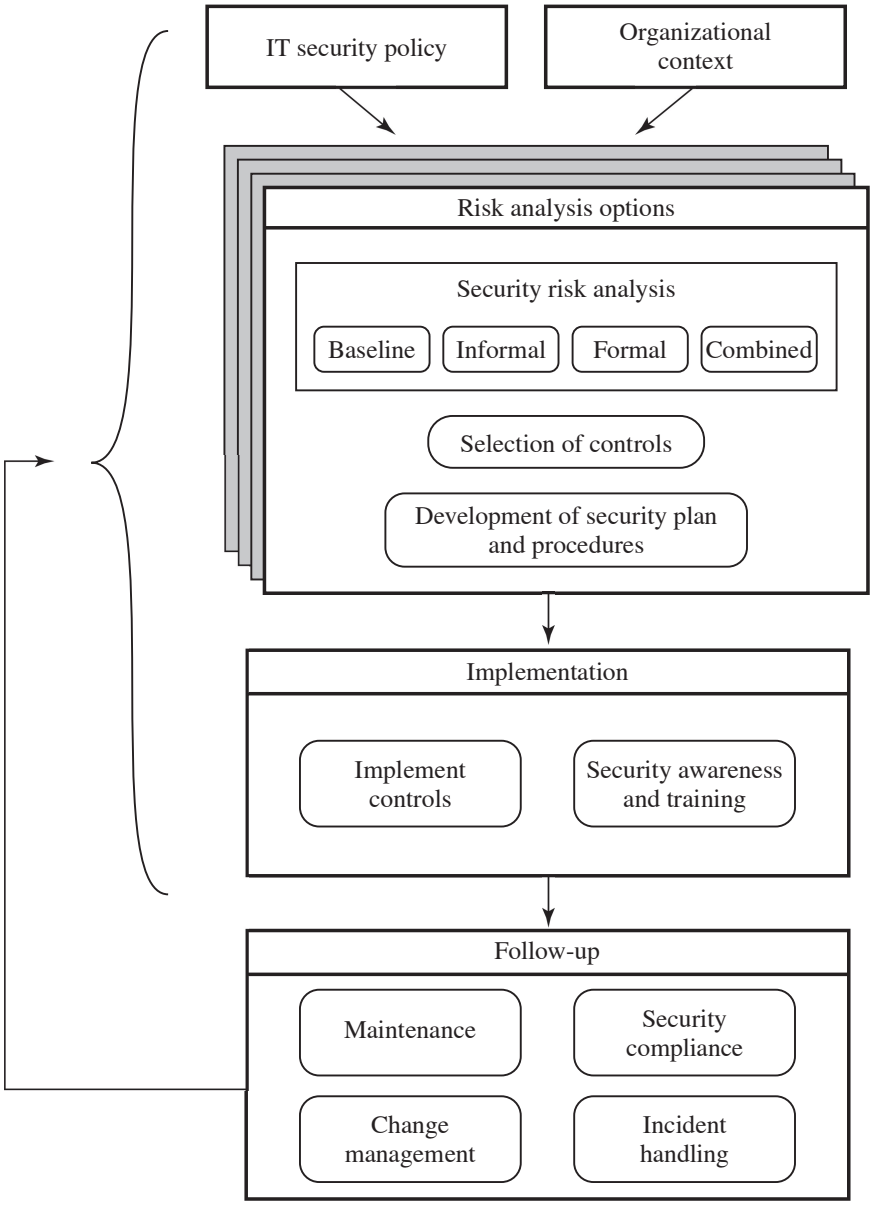

Figure 14.1 Overview of IT Security Management

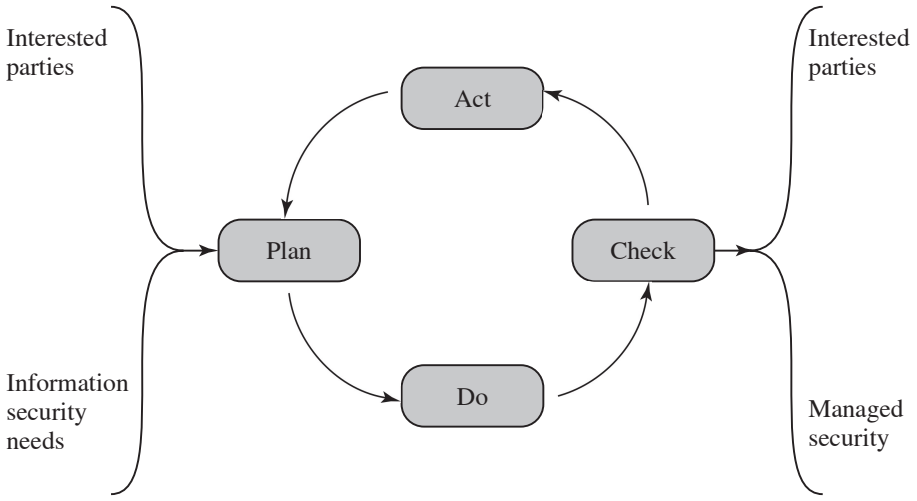

Figure 14.2 The Plan-Do-Check-Act Process Model

assessment of all the organization's assets and business processes. Hence, unless senior management in an organization are aware of, and support, this process, it is unlikely that the desired security objectives will be met and contribute appropriately to the organization's business outcomes. Note that IT management is not something undertaken just once. Rather it is a cyclic process that must be repeated constantly in order to keep pace with the rapid changes in both IT technology and the risk environment.

The iterative nature of this process is a key focus of ISO 31000 (*Risk management - Principles and guidelines*, 2009), and is specifically applied to the security risk management process in ISO 27005. This standard details a model process for managing information security that comprises the following steps:[1]

Plan: Establish security policy, objectives, processes, and procedures; perform risk assessment; develop risk treatment plan with appropriate selection of controls or acceptance of risk.

Do: Implement the risk treatment plan.

Check: Monitor and maintain the risk treatment plan.

Act: Maintain and improve the information security risk management process in response to incidents, review, or identified changes.

This process is illustrated in Figure 14.2, which can be aligned with Figure 14.1. The outcome of this process should be that the security needs of the interested parties are managed appropriately.

14.2 ORGANIZATIONAL CONTEXT AND SECURITY POLICY

The initial step in the IT security management process comprises an examination of the organization's IT security objectives, strategies, and policies in the context of the organization's general risk profile. This can only occur in the context of the wider

[1]Adapted from table 1 in ISO 27005 and part of figure 1 in ISO 31000.

organizational objectives and policies, as part of the management of the organization. Organizational security objectives identify what IT security outcomes should be achieved. They need to address individual rights, legal requirements, and standards imposed on the organization, in support of the overall organizational objectives. Organizational security strategies identify how these objectives can be met. Organizational security policies identify what needs to be done. These objectives, strategies, and policies need to be maintained and regularly updated based on the results of periodic security reviews to reflect the constantly changing technological and risk environments.

To help identify these organizational security objectives, the role and importance of the IT systems in the organization is examined. The value of these systems in assisting the organization achieve its goals is reviewed, not just the direct costs of these systems. Questions that help clarify these issues include the following:

- What key aspects of the organization require IT support in order to function efficiently?
- What tasks can only be performed with IT support?
- Which essential decisions depend on the accuracy, currency, integrity, or availability of data managed by the IT systems?
- What data created, managed, processed, and stored by the IT systems need protection?
- What are the consequences to the organization of a security failure in their IT systems?

If the answers to some of the above questions show that IT systems are important to the organization in achieving its goals, then clearly the risks to them should be assessed and appropriate action taken to address any deficiencies identified. A list of key organization security objectives should result from this examination.

Once the objectives are listed, some broad strategy statements can be developed. These outline in general terms how the identified objectives will be met in a consistent manner across the organization. The topics and details in the strategy statements depend on the identified objectives, the size of the organization, and the importance of the IT systems to the organization. The strategy statements should address the approaches the organization will use to manage the security of its IT systems.

Given the organizational security objectives and strategies, an **organizational security policy** is developed that describes what the objectives and strategies are and the process used to achieve them. The organizational or corporate security policy may be either a single large document or, more commonly, a set of related documents. This policy typically needs to address at least the following topics:[2]

- The scope and purpose of the policy
- The relationship of the security objectives to the organization's legal and regulatory obligations, and its business objectives
- IT security requirements in terms of confidentiality, integrity, availability, accountability, authenticity, and reliability, particularly with regard to the views of the asset owners

[2]Adapted from the details provided in various sections of ISO 13335.

- The assignment of responsibilities relating to the management of IT security and the organizational infrastructure
- The risk management approach adopted by the organization
- How security awareness and training is to be handled
- General personnel issues, especially for those in positions of trust
- Any legal sanctions that may be imposed on staff, and the conditions under which such penalties apply
- Integration of security into systems development and procurement
- Definition of the information classification scheme used across the organization
- Contingency and business continuity planning
- Incident detection and handling processes
- How and when this policy should be reviewed
- The method for controlling changes to this policy

The intent of the policy is to provide a clear overview of how an organization's IT infrastructure supports its overall business objectives in general, and more specifically, what security requirements must be provided in order to do this most effectively.

The term *security policy* is also used in other contexts. Previously, an organizational security policy referred to a document that detailed not only the overall security objectives and strategies, but also procedural policies that defined acceptable behavior, expected practices, and responsibilities. RFC 2196 (*Site Security Handbook*, 1997) describes this form of policy. This interpretation of a security policy predates the formal specification of IT security management as a process, as we describe in this chapter. Although the development of such a policy was expected to follow many of the steps we now detail as part of the IT security management process, there was much less detail in its description. The content of such a policy usually included many of the control areas described in standards such as ISO 27002, FIPS 200 and NIST SP 800-53, which we will explore further in Chapters 15–18.

A real-world example of such an organizational security policy, for an EU-based engineering consulting firm, is provided in the premium content section of this book's Website (ComputerSecurityPolicy.pdf). For our purposes, we have changed the name of the company to Company wherever it appears in this document. The company is an EU-based engineering consulting firm that specializes in the provision of planning, design, and management services for infrastructure development worldwide. As an illustration of the level of detail provided by this type of policy, Section 1 of the document SecurityPolicy.pdf, available at https://app.box.com/v/CompSec4e, reproduces Section 5 of the document, covering physical and environmental security.

Further guidance on requirements for a security policy is provided in online Section 2 of the document SecurityPolicy.pdf, which includes the specifications from *The Standard of Good Practice for Information Security* from the Information Security Forum.

The term *security policy* can also refer to specific security rules for specific systems, or to specific control procedures and processes. In the context of trusted computing, as we will discuss in Chapter 27, it refers to formal models for confidentiality and integrity. In this chapter though, we use the term to refer to the description of the overall security objectives and strategies, as described at the start of this section.

It is critical that an organization's IT security policy has full approval and buy-in by senior management. Without this, experience shows that it is unlikely that sufficient resources or emphasis will be given to meeting the identified objectives and achieving a suitable security outcome. With the clear, visible support of senior management, it is much more likely that security will be taken seriously by all levels of personnel in the organization. This support is also evidence of concern and due diligence in the management of the organization's systems and the monitoring of its risk profile.

Because the responsibility for IT security is shared across the organization, there is a risk of inconsistent implementation of security and a loss of central monitoring and control. The various standards strongly recommend that overall responsibility for the organization's IT security be assigned to a single person, the organizational IT security officer. This person should ideally have a background in IT security. The responsibilities of this person include:

- Oversight of the IT security management process.
- Liaison with senior management on IT security issues.
- Maintenance of the organization's IT security objectives, strategies, and policies.
- Coordination of the response to any IT security incidents.
- Management of the organization-wide IT security awareness and training programs.
- Interaction with IT project security officers.

Larger organizations will need separate IT project security officers associated with major projects and systems. Their role is to develop and maintain security policies for their systems, develop and implement security plans relating to these systems, handle the day-to-day monitoring of the implementation of these plans, and assist with the investigation of incidents involving their systems.

14.3 SECURITY RISK ASSESSMENT

We now turn to the key risk management component of the IT security process. This stage is critical, because without it there is a significant chance that resources will not be deployed where most effective. The result will be that some risks are not addressed, leaving the organization vulnerable, while other safeguards may be deployed without sufficient justification, wasting time and money. Ideally, every single organizational asset is examined, and every conceivable risk to it is evaluated. If a risk is judged to be too great, then appropriate remedial controls are deployed to reduce the risk to an acceptable level. In practice, this is clearly impossible. The time and effort required, even for large, well-resourced organizations, is clearly neither achievable nor cost effective. Even if possible, the rapid rate of change in both IT technologies and the wider threat environment means that any such assessment would be obsolete as soon as it is completed, if not earlier! Clearly some form of compromise evaluation is needed.

Another issue is the decision as to what constitutes an appropriate level of risk to accept. In an ideal world, the goal would be to eliminate all risks completely.

Again, this is simply not possible. A more realistic alternative is to expend an amount of resources in reducing risks proportional to the potential costs to the organization should that risk occur. This process also must take into consideration the likelihood of the risk's occurrence. Specifying the acceptable level of risk is simply prudent management and means that resources expended are reasonable in the context of the organization's available budget, time, and personnel resources. The aim of the risk assessment process is to provide management with the information necessary for them to make reasonable decisions on where available resources will be deployed.

Given the wide range of organizations, from very small businesses to global multinationals and national governments, there clearly needs to be a range of alternatives available in performing this process. There are a range of formal standards that detail suitable IT security risk assessment processes, including ISO 13335, ISO 27005, ISO 31000, and NIST SP 800-30. In particular, ISO 13335 recognizes four approaches to identifying and mitigating risks to an organization's IT infrastructure:

- Baseline approach
- Informal approach
- Detailed risk analysis
- Combined approach

The choice among these will be determined by the resources available to the organization and from an initial high-level risk analysis that considers how valuable the IT systems are and how critical to the organization's business objectives. Legal and regulatory constraints may also require specific approaches. This information should be determined when developing the organization's IT security objectives, strategies, and policies.

Baseline Approach

The baseline approach to risk assessment aims to implement a basic general level of security controls on systems using baseline documents, codes of practice, and *industry best practice*. The advantages of this approach are that it does not require the expenditure of additional resources in conducting a more formal risk assessment and that the same measures can be replicated over a range of systems. The major disadvantage is that no special consideration is given to variations in the organization's risk exposure based on who they are and how their systems are used. In additional, there is a chance that the baseline level may be set either too high, leading to expensive or restrictive security measures that may not be warranted, or set too low, resulting in insufficient security and leaving the organization vulnerable.

The goal of the baseline approach is to implement generally agreed controls to provide protection against the most common threats. These would include implementing industry best practice in configuring and deploying systems, like those we discussed, in Chapter 12 on operating systems security. As such, the baseline approach forms a good base from which further security measures can be determined. Suitable baseline recommendations and checklists may be obtained from a range of organizations, including:

- Various national and international standards organizations
- Security-related organizations such as the CERT, NSA, and so on
- Industry sector councils or peak groups

The use of the baseline approach alone would generally be recommended only for small organizations without the resources to implement more structured approaches. But it will at least ensure that a basic level of security is deployed, which is not guaranteed by the default configurations of many systems.

Informal Approach

The informal approach involves conducting some form of informal, pragmatic risk analysis for the organization's IT systems. This analysis does not involve the use of a formal, structured process, but rather exploits the knowledge and expertise of the individuals performing this analysis. These may either be internal experts, if available, or alternatively, external consultants. A major advantage of this approach is that the individuals performing the analysis require no additional skills. Hence, an informal risk assessment can be performed relatively quickly and cheaply. In addition, because the organization's systems are being examined, judgments can be made about specific vulnerabilities and risks to systems for the organization that the baseline approach would not address. Thus, more accurate and targeted controls may be used than would be the case with the baseline approach. There are a number of disadvantages. Because a formal process is not used, there is a chance that some risks may not be considered appropriately, potentially leaving the organization vulnerable. Besides, because the approach is informal, the results may be skewed by the views and prejudices of the individuals performing the analysis. It may also result in insufficient justification for suggested controls, leading to questions over whether the proposed expenditure is really justified. Lastly, there may be inconsistent results over time as a result of differing expertise in those conducting the analysis.

The use of the informal approach would generally be recommended for small to medium-sized organizations where the IT systems are not necessarily essential to meeting the organization's business objectives, and where additional expenditure on risk analysis cannot be justified.

Detailed Risk Analysis

The third and most comprehensive approach is to conduct a detailed risk assessment of the organization's IT systems, using a formal structured process. This provides the greatest degree of assurance that all significant risks are identified and their implications considered. This process involves a number of stages, including identification of assets, identification of threats and vulnerabilities to those assets, determination of the likelihood of the risk occurring and the consequences to the organization should that occur, and hence the risk to which the organization is exposed. With that information, appropriate controls can be chosen and implemented to address the risks identified. The advantages of this approach are that it provides the most detailed examination of the security risks of an organization's IT system, and produces strong justification for expenditure on the controls proposed. It also provides the best information for continuing to manage the security of these systems as they evolve and change. The major disadvantage is the significant cost in time, resources, and expertise needed to perform such an analysis. The time taken to perform this analysis may also result in delays in providing suitable levels of

protection for some systems. The details of this approach will be discussed in the next section.

The use of a formal, detailed risk analysis is often a legal requirement for some government organizations and businesses providing key services to them. This may also be the case for organizations providing key national infrastructure. For such organizations, there is no choice but to use this approach. It may also be the approach of choice for large organizations with IT systems critical to their business objectives and with the resources available to perform this type of analysis.

Combined Approach

The last approach combines elements of the baseline, informal, and detailed risk analysis approaches. The aim is to provide reasonable levels of protection as quickly as possible then to examine and adjust the protection controls deployed on key systems over time. The approach starts with the implementation of suitable baseline security recommendations on all systems. Next, systems either exposed to high risk levels or critical to the organization's business objectives are identified in the high-level risk assessment. A decision can then be made to possibly conduct an immediate informal risk assessment on key systems, with the aim of relatively quickly tailoring controls to more accurately reflect their requirements. Lastly, an ordered process of performing detailed risk analyses of these systems can be instituted. Over time, this can result in the most appropriate and cost-effective security controls being selected and implemented on these systems. This approach has a significant number of advantages. The use of the initial high-level analysis to determine where further resources need to be expended, rather than facing a full detailed risk analysis of all systems, may well be easier to sell to management. It also results in the development of a strategic picture of the IT resources and where major risks are likely to occur. This provides a key planning aid in the subsequent management of the organization's security. The use of the baseline and informal analyses ensures that a basic level of security protection is implemented early. Resources are likely to be applied where most needed, and systems most at risk are likely to be examined further reasonably early in the process. However, there are some disadvantages. If the initial high-level analysis is inaccurate, then some systems for which a detailed risk analysis should be performed may remain vulnerable for some time. Nonetheless, the use of the baseline approach should ensure a basic minimum security level on such systems. Further, if the results of the high-level analysis are reviewed appropriately, the chance of lingering vulnerability is minimized.

ISO 13335 considers that for most organizations, in most circumstances, this approach is the most cost effective. Consequently, its use is highly recommended.

14.4 DETAILED SECURITY RISK ANALYSIS

The formal, detailed security risk analysis approach provides the most accurate evaluation of an organization's IT system's security risks, but at the highest cost. This approach has evolved with the development of trusted computer systems, initially