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 the organization is exposed to. 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 are 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, and 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. And it means that resources are likely to be applied where most needed and that 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.

[ISO13335] 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 focused on addressing defense security concerns, as we discuss in Chapter 13. The original security risk assessment methodology was given in the Yellow Book standard (CSC-STD-004-85 June 1985), one of the original U.S. TCSEC rainbow book series of standards. Its focus was entirely on protecting the confidentiality of information, reflecting the military concern with information classification. The recommended rating it gave for a trusted computer system depended on difference between the minimum user clearance and the maximum information classification. Specifically it defined a risk index as

$$\text{Risk Index} = \text{Max Info Sensitivity} - \text{Min User Clearance}$$

A table in this standard, listing suitable categories of systems for each risk level, was used to select the system type. Clearly this limited approach neither adequately reflects the range of security services required nor the wide range of possible threats. Over the years since, the process of conducting a security risk assessment that does consider these issues has evolved.

A number of national and international standards document the expected formal risk analysis approach. These include [ISO27005], [NIST12], [ISO31000], [SASN06], and [SA04]. This approach is often mandated by government organizations and associated businesses. These standards all broadly agree on the process used. Figure 14.3 (reproduced from figure 5 in [NIST12]) illustrates a typical process used.

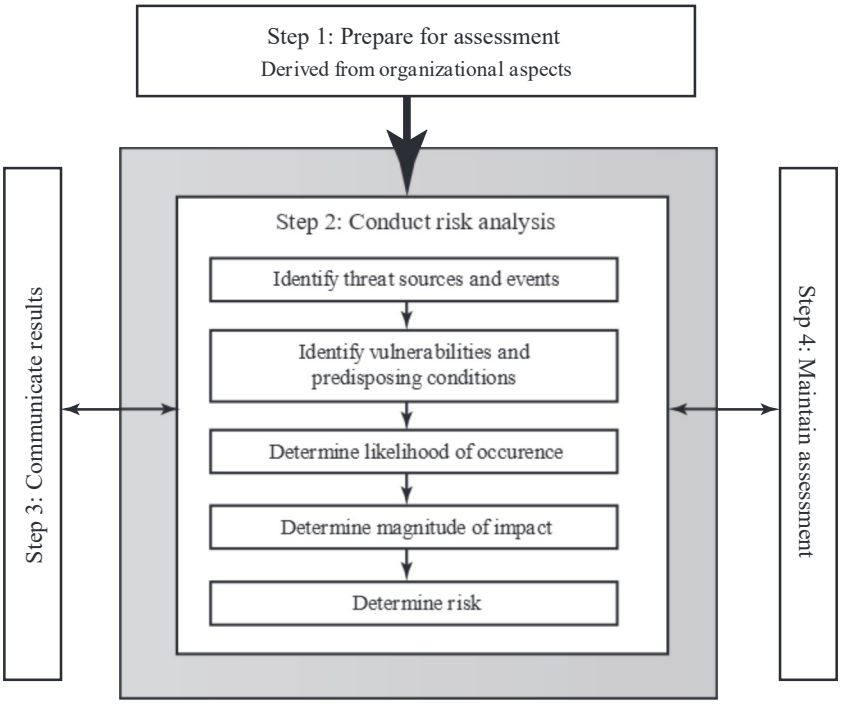

Figure 14.3 **Risk Assessment Process**

Context and System Characterization

The initial step is known as *establishing the context* or *system characterization*. Its purpose is to determine the basic parameters within which the risk assessment will be conducted, and then to identify the assets to be examined.

Establishing the Context The process starts with the organizational security objectives and considers the broad risk exposure of the organization. This recognizes that not all organizations are equally at risk, but that some, because of their function, may be specifically targeted. It explores the relationship between a specific organization and the wider political and social environment in which it operates. Figure 14.4 (adapted from an IDC 2000 report) suggests a possible spectrum of organizational risk. Industries such as agriculture and education are considered to be at lesser risk compared to government or banking and finance. Note that this classification predates September 11, and it is likely that there has been change since it was developed. In particular it is likely that utilities, for example, are probably at higher risk than the classification suggests. NIST has indicated[3] that the following industries are vulnerable to risks in Supervisory Control and Data Acquisition (SCADA) and process control systems: electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods), air and rail transportation, and mining and metallurgy.

At this point in determining an organization's broad risk exposure, any relevant legal and regulatory constraints must also be identified. These features provide a baseline for the organization's risk exposure and an initial indication of the broad scale of resources it needs to expend to manage this risk in order to successfully conduct business.

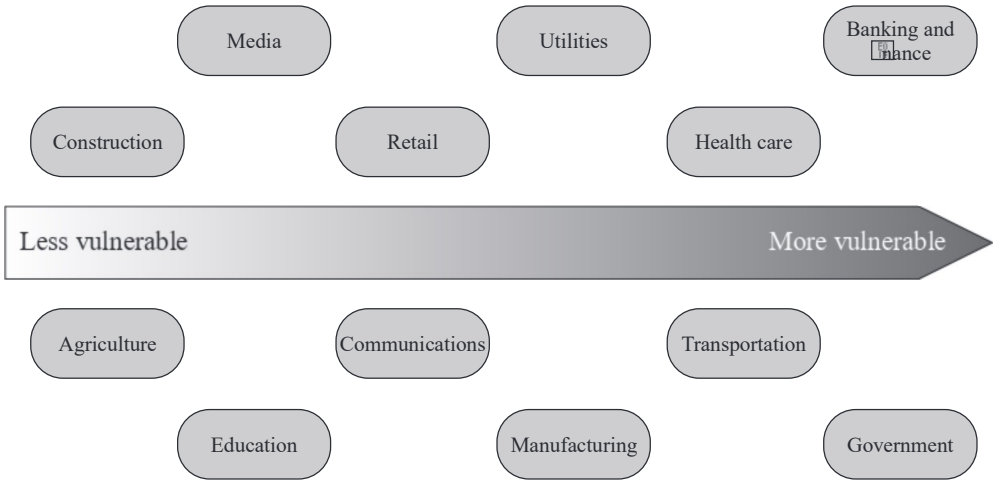

Figure 14.4 Generic Organizational Risk Context

[3]Adapted from the Executive Summary of [NIST13].

Next, senior management must define the organization's **risk appetite**, the level of risk the organization views as acceptable. Again this will depend very much on the type of organization, and its management's attitude to how it conducts business. For example, banking and finance organizations tend to be fairly conservative and risk averse. This means they want a low residual risk and are willing to spend the resources necessary to achieve this. In contrast, a leading-edge manufacturer with a brand new product may have a much greater risk tolerance. The manufacturer is willing to take a chance to obtain a competitive advantage, and with limited resources wishes to expend less on risk controls. This decision is not just IT specific. Rather it reflects the organization's broader management approach to how it conducts business.

The boundaries of this risk assessment are then identified. This may range from just a single system or aspect of the organization to its entire IT infrastructure. This will depend in part on the risk assessment approach being used. A combined approach requires separate assessments of critical components over time as the security profile of the organization evolves. It also recognizes that not all systems may be under control of the organization. In particular, if services or systems are provided externally, they may need to be considered separately. The various stakeholders in the process also need to be identified, and a decision must be made as to who conducts and monitors the risk assessment process for the organization. Resources must be allocated for the process. This all requires support from senior management, whose commitment is critical for the successful completion of the process.

A decision also needs to be made as to precisely which risk assessment criteria will be used in this process. While there is broad general agreement on this process, the actual details and tables used vary considerably and are still evolving. This decision may be determined by what has been used previously in this, or related, organizations. For government organizations, this decision may be specified by law or regulation. Lastly the knowledge and experience of those performing the analysis may determine the criteria used.

Asset Identification The last component of this first step in the risk assessment is to identify the assets to examine. This directly addresses the first of the three fundamental questions we opened this chapter with: "What assets do we need to protect?" An **asset** is "anything that needs to be protected" because it has value to the organization and contributes to the successful attainment of the organization's objectives. As we discuss in Chapter 1, an asset may be either tangible or intangible. It includes computer and communications hardware infrastructure, software (including applications and information/data held on these systems), the documentation on these systems, and the people who manage and maintain these systems. Within the boundaries identified for the risk assessment, these assets need to be identified and their value to the organization assessed. It is important to emphasize again that while the ideal is to consider every conceivable asset, in practice this is not possible. Rather the goal here is to identify all assets that contribute significantly to attaining the organization's objectives and whose compromise or loss would seriously impact on the organization's operation. [SASN06] describes this process as a criticality assessment that aims to identify those assets that are most important to the organization.

While the risk assessment process is most likely being managed by security experts, they will not necessarily have a high degree of familiarity with the organization's operation and structures. Thus they need to draw on the expertise of the people in the relevant areas of the organization to identify key assets and their value to the organization. A key element of this process step is identifying and interviewing such personnel. Many of the standards listed previously include checklists of types of assets and suggestions for mechanisms for gathering the necessary information. These should be consulted and used. The outcome of this step should be a list of assets, with brief descriptions of their use by, and value to, the organization.

Identification of Threats/Risks/Vulnerabilities

The next step in the process is to identify the threats or risks the assets are exposed to. This directly addresses the second of our three fundamental questions: "How are those assets threatened?" It is worth commenting on the terminology used here. The terms *threat* and *risk*, while having distinct meanings, are often used interchangeably in this context. There is considerable variation in the definitions of these terms, as seen in the range of definitions provided in the cited standards. The following definitions will be useful in our discussion:

Asset:	A system resource or capability of value to its owner that requires protection.
Threat:	A potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner.
Vulnerability:	A flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat.
Risk:	The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner.

The relationship among these and other security concepts is illustrated in Figure 1.2, which shows that central term risk results from a threat exploiting vulnerabilities in assets that causes loss of value to the organization.

The goal of this stage is to identify potentially significant risks to the assets listed. This requires answering the following questions for each asset:

1. Who or what could cause it harm?
2. How could this occur?

threat identification Answering the first of these questions involves identifying potential threats to assets. In the broadest sense, a **threat** is anything that might hinder or prevent an asset from providing appropriate levels of the key security services: confidentiality, integrity, availability, accountability, authenticity, and reliability. Note that one asset may have multiple threats, and a single threat may target multiple assets.

A threat may be either natural or human-made and may be accidental or deliberate. This is known as the **threat source**. The classic natural threat sources are those often referred to as acts of God, and include damage caused by fire, flood, storm, earthquake, and other such natural events. It also includes environmental threats such as long-term loss of power or natural gas. Or it may be the result of chemical contamination or leakage. Alternatively, a threat source may be a human agent acting either directly or indirectly. Examples of the former include an insider retrieving and selling information for personal gain or a hacker targeting the organization's server over the Internet. An example of the latter includes someone writing and releasing a network worm that infects the organization's systems. These examples all involved a deliberate exploit of a threat. However, a threat may also be a result of an accident, such as an employee incorrectly entering information on a system, which results in the system malfunctioning.

Identifying possible threats and threat sources requires the use of a variety of sources, along with the experience of the risk assessor. The chance of natural threats occurring in any particular area is usually well known from insurance statistics. Lists of other potential threats may be found in the standards, in the results of IT security surveys, and in information from government security agencies. The annual computer crime reports, such as those by CSI/FBI and by Verizon in the United States, and similar reports in other countries, provide useful general guidance on the broad IT threat environment and the most common problem areas. Standards, such as [NIST12] Appendix D with a taxonomy of threat sources, and Appendix E with examples of threats, may also assist here.

However, this general guidance needs to be tailored to the organization and the risk environment it operates in. This involves consideration of vulnerabilities in the organization's IT systems, which may indicate that some risks are either more or less likely than the general case. Where an organization's security concerns are sufficiently high that threats need to be specifically identified, threat scenarios can be modelled, developed, and analyzed, as described in [NIST12]. Organization's define threat scenarios to describe how the tactics, techniques, and procedures employed by an attacker can contribute to, or cause, harm. The possible motivation of deliberate attackers in relation to the organization should be considered as potentially influencing this variation in risk. In addition, any previous experience of attacks seen by the organization needs to be considered, as that is concrete evidence of risks that are known to occur. When evaluating possible human threat sources, it is worth considering their reason and capabilities for attacking this organization, including their:

- **Motivation:** Why would they target this organization; how motivated are they?
- **Capability:** What is their level of skill in exploiting the threat?
- **Resources:** How much time, money, and other resources could they deploy?
- **Probability of attack:** How likely and how often would your assets be targeted?
- **Deterrence:** What are the consequences to the attacker of being identified?

Vulnerability Identification Answering the second of these questions, "How could this occur?" involves identifying flaws or weaknesses in the organization's

IT systems or processes that could be exploited by a threat source. This will help determine the applicability of the threat to the organization and its significance. Note that the mere existence of some vulnerability does not mean harm will be caused to an asset. There must also be a threat source for some threat that can exploit the vulnerability for harm. It is the combination of a threat and a vulnerability that creates a risk to an asset.

Again, many of the standards listed previously include checklists of threats and vulnerabilities and suggestions for tools and techniques to list them and to determine their relevance to the organization. The outcome of this step should be a list of threats and vulnerabilities, with brief descriptions of how and why they might occur.

Analyze Risks

Having identified key assets and the likely threats and vulnerabilities they are exposed to, the next step is to determine the level of risk each of these poses to the organization. The aim is to identify and categorize the risks to assets that threaten the regular operations of the organization. Risk analysis also provides information to management to help managers evaluate these risks and determine how best to treat them. Risk analysis involves first specifying the likelihood of occurrence of each identified threat to an asset, in the context of any existing controls. Next, the consequence to the organization is determined, should that threat eventuate. Lastly, this information is combined to derive an overall risk rating for each threat. The ideal would be to specify the likelihood as a probability value and the consequence as a monetary cost to the organization should it occur. The resulting risk is then simply given as

$$\text{Risk} = (\text{Probability that threat occurs}) * (\text{Cost to organization})$$

This can be directly equated to the value the threatened asset has for the organization, and hence specify what level of expenditure is reasonable to reduce the probability of its occurrence to an acceptable level. Unfortunately, it is often extremely hard to determine accurate probabilities, realistic cost consequences, or both. This is particularly true of intangible assets, such as the loss of confidentiality of a trade secret. Hence, most risk analyses use qualitative, rather than quantitative, ratings for both these items. The goal is then to order the resulting risks to help determine which need to be most urgently treated, rather than to give them an absolute value.

Analyze Existing Controls Before the likelihood of a threat can be specified, any existing controls used by the organization to attempt to minimize threats need to be identified. Security **controls** include management, operational, and technical processes and procedures that act to reduce the exposure of the organization to some risks by reducing the ability of a threat source to exploit some vulnerabilities. These can be identified by using checklists of existing controls, and by interviewing key organizational staff to solicit this information.

Table 14.2 Risk Likelihood

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may be deemed as "unlucky" or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

d Et Er min E l ik El ih o o d Having identified existing controls, the **likelihood** that each identified threat could occur and cause harm to some asset needs to be specified. The likelihood is typically described qualitatively, using values and descriptions such as those shown in Table 14.2.[4] While the various risk assessment standards all suggest tables similar to these, there is considerable variation in their detail.[5] The selection of the specific descriptions and tables used is determined at the beginning of the risk assessment process, when the context is established.

There will very likely be some uncertainty and debate over exactly which rating is most appropriate. This reflects the qualitative nature of the ratings, ambiguity in their precise meaning, and uncertainty over precisely how likely it is that some threat may eventuate. It is important to remember that the goal of this process is to provide guidance to management as to which risks exist, and provide enough information to help management decide how to most appropriately respond. Any uncertainty in the selection of ratings should be noted in the discussion on their selection, but ultimately management will make a business decision in response to this information.

The risk analyst takes the descriptive asset and threat/vulnerability details from the preceding steps in this process and, in light of the organization's overall risk environment and existing controls, decides the appropriate rating. This estimation relates to the likelihood of the specified threat exploiting one or more vulnerabilities to an asset or group of assets, which results in harm to the organization. When deliberate human-made threat sources are considered, this estimate should include an evaluation of the attackers intent, capability, and specific targeting of this organization. The specified likelihood needs to be realistic. In particular, a rating of likely or higher suggests that this threat has occurred sometime previously. This means past history provides supporting evidence for its

[4]This table, along with Tables 16.3 and 16.4, is adapted from those given in [ISO27005], [ISO31000], [SASN06], and [SA04], but with descriptions expanded and generalized to apply to a wider range of organizations.

[5]The tables used in this chapter are chosen to illustrate a more detailed level of analysis than used in some other standards.

specification. If this is not the case, then specifying such a value would need to be justified on the basis of a significantly changed threat environment, a change in the IT system that has weakened its security, or some other rationale for the threat's anticipated likely occurrence. In contrast, the Unlikely and Rare ratings can be very hard to quantify. They are an indication that the threat is of concern, but whether it could occur is difficult to specify. Typically such threats would only be considered if the consequences to the organization of their occurrence are so severe that they must be considered, even if extremely improbable.

Determine Consequence/Impact on Organization The analyst must then specify the consequence of a specific threat eventuating. Note this is distinct from, and not related to, the likelihood of the threat occurring. Rather, **consequence** specification indicates the impact on the organization should the particular threat in question actually eventuate. Even if a threat is regarded as rare or unlikely, if the organization would suffer severe consequence should it occur, then it clearly poses a risk to the organization. Hence, appropriate responses must be considered. A qualitative descriptive value, such as those shown in Table 14.3, is typically used to describe the consequence. As with the likelihood ratings, there is likely to be some uncertainty as to the best rating to use.

This determination should be based upon the judgment of the asset's owners, and the organization's management, rather than the opinion of the risk analyst. This is in contrast with the likelihood determination. The specified consequence needs to be realistic. It must relate to the impact on the organization as a whole should this specific threat eventuate. It is not just the impact on the affected system. It is possible that a particular system (a server in one location, for example) might be completely destroyed in a fire. However, the impact on the organization could vary from it being a minor inconvenience (the server was in a branch office, and all data were

Table 14.3 Risk Consequences

Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. Usually does not result in any tangible detriment to the organization.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. Again, does not result in any tangible detriment to the organization, but may, in hindsight, show previous lost opportunities or lack of efficiency.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and will generally require management intervention, though should still be able to be dealt with at the project or team level. Will require some ongoing compliance costs to overcome. Customers or the public may be indirectly aware or have limited information about this event.

(Continued)

Table 14.3 (Continued)

Rating	Consequence	Expanded Definition
4	**Major**	Ongoing systemic security breach. Impact will likely last 4–8 weeks and require significant management intervention and resources to overcome. Senior management will be required to sustain ongoing direct management for the duration of the incident and compliance costs are expected to be substantial. Customers or the public will be aware of the occurrence of such an event and will be in possession of a range of important facts. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. A loss of customer business or other significant harm to the organization is expected. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action against personnel involved is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable. Compliance costs are likely to result in annual losses for some years, with liquidation of the organization likely.

replicated elsewhere) to a major disaster (the server had the sole copy of all customer and financial records for a small business). As with the likelihood ratings, the consequence ratings must be determined knowing the organization's current practices and arrangements. In particular, the organization's existing backup, disaster recovery, and contingency planning, or lack thereof, will influence the choice of rating.

Determining Resulting Level of Risk Once the likelihood and consequence of each specific threat have been identified, a final **level of risk** can be assigned. This is typically determined using a table that maps these values to a risk level, such as those shown in Table 14.4. This table details the risk level assigned to each combination. Such a table provides the qualitative equivalent of performing the ideal risk calculation using quantitative values. It also indicates the interpretation of these assigned levels.

Documenting the Results in a Risk Register The results of the risk analysis process should be documented in a **risk register**. This should include a summary table such that shown in Table 14.5. The risks are usually sorted in decreasing order of level. This would be supported by details of how the various items were determined, including the rationale, justification, and supporting evidence used. The aim of this documentation is to provide senior management with the information needed to make appropriate decisions as how to best manage the identified risks. It also provides evidence that a formal risk assessment process

Table 14.4 Risk Level Determination and Meaning

	Consequences					
Likelihood	**Doomsday**	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk is expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls is likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

has been followed if needed, and a record of decisions made with the reasons for those decisions.

Evaluate Risks

Once the details of potentially significant risks are determined, management needs to decide whether it needs to take action in response. This would take into account the risk profile of the organization and its willingness to accept a certain level of risk, as determined in the initial *establishing the context* phase of this process. Those items with risk levels below the acceptable level would usually be accepted with no further action required. Those items with risks above this will need to be considered for treatment.

Table 14.5 Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet router	Outside hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of data center	Accidental fire or flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Risk Treatment

Typically the risks with the higher ratings are those that need action most urgently. However, it is likely that some risks will be easier, faster, and cheaper to address than others. In the example risk register shown in Table 14.5, both risks were rated High. Further investigation reveals that a relatively simple and cheap treatment exists for the first risk by tightening the router configuration to further restrict possible accesses. Treating the second risk requires developing a full disaster recovery plan, a much slower and more costly process. Hence management would take the simple action first to improve the organization's overall risk profile as quickly as possible. Management may even decide that for business reasons, given an overall view of the organization, some risks with lower levels should be treated ahead of other risks. This is a reflection of both limitations in the risk analysis process in the range of ratings available and their interpretation, and of management's perspective of the organization as a whole.

Figure 14.5 indicates a range of possibilities for costs versus levels of risk. If the cost of treatment is high, but the risk is low, then it is usually uneconomic to proceed with such treatment. Alternatively, where the risk is high and the cost comparatively low, treatment should occur. The most difficult area occurs between these extremes. This is where management must make a business decision about the most effective use of their available resources. This decision usually requires a more detailed investigation of the treatment options. There are five broad alternatives available to management for treating identified risks:

- **Risk acceptance:** Choosing to accept a risk level greater than normal for business reasons. This is typically due to excessive cost or time needed to treat the

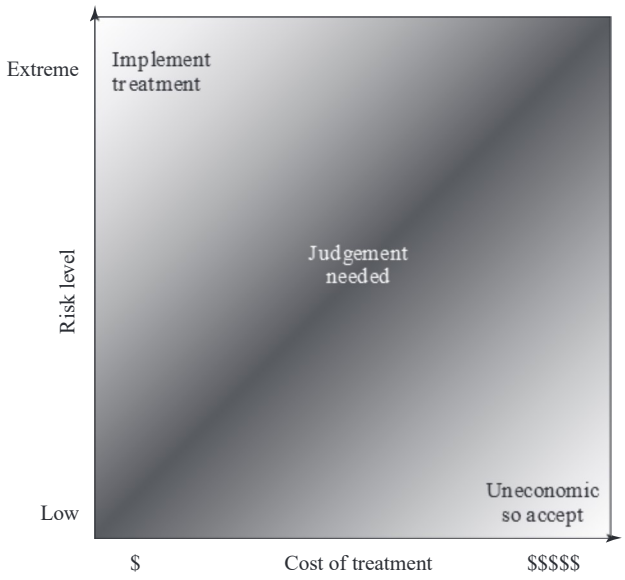

Figure 14.5 Judgment about Risk Treatment

risk. Management must then accept responsibility for the consequences to the organization should the risk eventuate.

- **Risk avoidance:** Not proceeding with the activity or system that creates this risk. This usually results in loss of convenience or ability to perform some function that is useful to the organization. The loss of this capability is traded off against the reduced risk profile.
- **Risk transfer:** Sharing responsibility for the risk with a third party. This is typically achieved by taking out insurance against the risk occurring, by entering into a contract with another organization, or by using partnership or joint venture structures to share the risks and costs should the threat eventuate.
- **Reduce consequence:** By modifying the structure or use of the assets at risk to reduce the impact on the organization should the risk occur. This could be achieved by implementing controls to enable the organization to quickly recover should the risk occur. Examples include implementing an off-site backup process, developing a disaster recovery plan, or arranging for data and processing to be replicated over multiple sites.
- **Reduce likelihood:** By implementing suitable controls to lower the chance of the vulnerability being exploited. These could include technical or administrative controls such as deploying firewalls and access tokens, or procedures such as password complexity and change policies. Such controls aim to improve the security of the asset, making it harder for an attack to succeed by reducing the vulnerability of the asset.

If either of the last two options is chosen, then possible treatment controls need to be selected and their cost effectiveness evaluated. There is a wide range of available management, operational, and technical controls that may be used. These would be surveyed to select those that might address the identified threat most effectively and to evaluate the cost to implement against the benefit gained. Management would then choose among the options as to which should be adopted and plan for their implementation. We introduce the range of controls often used and the use of security plans and policies in Chapter 15 and provide further details of some specific control areas in Chapters 16–18.

14.5 Case Study: Silver Star Mines

A case study involving the operations of a fictional company Silver Star Mines illustrates this risk assessment process.[6] Silver Star Mines is the local operations of a large global mining company. It has a large IT infrastructure used by numerous business areas. Its network includes a variety of servers, executing a range of application software typical of organizations of its size. It also uses applications that are far less common, some of which directly relate to the health and safety of those working in the mine. Many of these systems used to be isolated, with no network connections among them.

[6]This example has been adapted and expanded from a 2003 study by Peter Hoek. For our purposes, the name of the original company and any identifying details have been changed.

In recent years, they have been connected together and connected to the company's intranet to provide better management capabilities. However, this means they are now potentially accessible from the Internet, which has greatly increased the risks to these systems.

A security analyst was contracted to provide an initial review of the company's risk profile and to recommend further action for improvement. Following initial discussion with company management, a decision was made to adopt a *combined approach* to security management. This requires the adoption of suitable baselines standards by the company's IT support group for their systems. Meanwhile, the analyst was asked to conduct a preliminary formal assessment of the key IT systems to identify those most at risk, which management could then consider for treatment.

The first step was to determine the context for the risk assessment. Being in the mining industry sector places the company at the less risky end of the spectrum, and consequently less likely to be specifically targeted. Silver Star Mines is part of a large organization and hence is subject to legal requirements for occupational health and safety and is answerable to its shareholders. Thus management decided that it wished to accept only moderate or lower risks in general. The boundaries for this risk assessment were specified to include only the systems under the direct control of the Silver Star Mines operations. This excluded the wider company intranet, its central servers, and its Internet gateway. This assessment is sponsored by Silver Star's IT and engineering managers, with results to be reported to the company board. The assessment would use the process and ratings described in this chapter.

Next, the key assets had to be identified. The analyst conducted interviews with key IT and engineering managers in the company. A number of the engineering managers emphasized how important the reliability of the SCADA network and nodes were to the company. They control and monitor the core mining operations of the company and enable it to operate safely and efficiently and, most crucially, to generate revenue. Some of these systems also maintain the records required by law, which are regularly inspected by the government agencies responsible for the mining industry. Any failure to create, preserve, and produce on demand these records would expose the company to fines and other legal sanctions. Hence, these systems were listed as the first key asset.

A number of the IT managers indicated that a large amount of critical data was stored on various file servers either in individual files or in databases. They identified the importance of the integrity of these data to the company. Some of these data were generated automatically by applications. Other data were created by employees using common office applications. Some of this needed to be available for audits by government agencies. There were also data on production and operational results, contracts and tendering, personnel, application backups, operational and capital expenditure, mine survey and planning, and exploratory drilling. Collectively, the integrity of stored data was identified as the second key asset.

These managers also indicated that three key systems—the Financial, Procurement, and Maintenance/Production servers—were critical to the effective operation of core business areas. Any compromise in the availability or integrity

of these systems would impact the company's ability to operate effectively. Hence each of these were identified as a key asset.

Lastly, the analyst identified e-mail as a key asset, as a result of interviews with all business areas of the company. The use of e-mail as a business tool cuts across all business areas. Around 60% of all correspondence is in the form of e-mail, which is used to communicate daily with head office, other business units, suppliers, and contractors, as well as to conduct a large amount of internal correspondence. E-mail is given greater importance than usual due to the remote location of the company. Hence the collective availability, integrity, and confidentiality of mail services was listed as a key asset.

This list of key assets is seen in the first column of Table 14.6, which is the risk register created at the conclusion of this risk assessment process.

Having determined the list of key assets, the analyst needed to identify significant threats to these assets and to specify the likelihood and consequence values. The major concern with the SCADA asset is unauthorized compromise of nodes by an external source. These systems were originally designed for use on physically isolated and trusted networks and hence were not hardened against external attack to the degree that modern systems can be. Often these systems are running

Table 14.6 Silver Star Mines—Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	Layered firewalls and servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	Firewall, policies	Possible	Major	Extreme	2
Availability and integrity of financial system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	3
Availability and integrity of procurement system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	4
Availability and integrity of maintenance/ production system	Attacks/errors affecting system	Firewall, policies	Possible	Minor	Medium	5
Availability, integrity, and confidentiality of mail services	Attacks/errors affecting system	Firewall, ext mail gateway	Almost Certain	Minor	High	6

older releases of operating systems with known insecurities. Many of these systems have not been patched or upgraded because the key applications they run have not been updated or validated to run on newer OS versions. More recently, the SCADA networks have been connected to the company's intranet to provide improved management and monitoring capabilities. Recognizing that the SCADA nodes are very likely insecure, these connections are isolated from the company intranet by additional firewall and proxy server systems. Any external attack would have to break through the outer company firewall, the SCADA network firewall, and these proxy servers in order to attack the SCADA nodes. This would require a series of security breaches. Nonetheless, given that the various computer crime surveys suggest that externally sourced attacks are increasing and known cases of attacks on SCADA networks exist, the analyst concluded that while an attack was very unlikely, it could still occur. Thus a likelihood rating of Rare was chosen. The consequence of the SCADA network suffering a successful attack was discussed with the mining engineers. They indicated that interference with the control system could have serious consequences as it could affect the safety of personnel in the mine. Ventilation, bulk cooling, fire protection, hoisting of personnel and materials, and underground fill systems are possible areas whose compromise could lead to a fatality. Environmental damage could result from the spillage of highly toxic materials into nearby waterways. Additionally, the financial impact could be significant, as downtime is measured in tens of millions of dollars per hour. There is even a possibility that Silver Star's mining license might be suspended if the company was found to have breached its legal requirements. A consequence rating of Major was selected. This results in a risk level of High.

The second asset concerned the integrity of stored information. The analyst noted numerous reports of unauthorized use of file systems and databases in recent computer crime surveys. These assets could be compromised by both internal and external sources. These can be either the result of intentional malicious or fraudulent acts, or the unintentional deletion, modification, or disclosure of information. All indications are that such database security breaches are increasing and that access to such data is a primary goal of intruders. These systems are located on the company intranet and hence are shielded by the company's outer firewall from much external access. However, should that firewall be compromised or an attacker gain indirect access using infected internal systems, compromise of the data was possible. With respect to internal use, the company had policies on the input and handling of a range of data, especially that required for audit purposes. The company also had policies on the backup of data from servers. However, the large number of systems used to create and store this data, both desktop and server, meant that overall compliance with these policies was unknown. Hence a likelihood rating of Possible was chosen. Discussions with some of the company's IT managers revealed that some of this information is confidential and may cause financial harm if disclosed to others. There also may be substantial financial costs involved with recovering data and other activities subsequent to a breach. There is also the possibility of serious legal consequences if personal information was disclosed or if the results of statutory tests and process information were lost. Hence a consequence rating of Major was selected. This results in a risk level of Extreme.

The availability or integrity of the key Financial, Procurement, and Maintenance/Production systems could be compromised by any form of attack on the operating system or applications they use. Although their location on the company intranet does provide some protection, due to the nature of the company structure a number of these systems have not been patched or maintained for some time. This means at least some of the systems would be vulnerable to a range of network attacks if accessible. Any failure of the company's outer firewall to block any such attack could very likely result in compromise of some systems by automated attack scans. These are known to occur very quickly, with a number of reports indicating that unpatched systems were compromised in less than 15 minutes after network connection. Hence a likelihood of Possible was specified. Discussions with management indicated that the degree of harm would be proportional to extent and duration of the attack. In most cases a rebuild of at least a portion of the system would be required, at considerable expense. False orders being issued to suppliers or the inability to issue orders would have a negative impact on the company's reputation and could cause confusion and possible plant shutdowns. Not being able to process personnel time sheets and utilize electronic funds transfer and unauthorized transfer of money would also affect the company's reputation and possibly result in a financial loss. The company indicated that the Maintenance/Production system's harm rating should be a little lower due the ability of the plant to continue to operate despite some compromise of the system. It would, however, have a detrimental impact on the efficiency of operations. Consequence ratings of Moderate and Minor, respectively, were selected, resulting in risk levels of High or Medium.

The last asset is the availability, integrity, and confidentiality of mail services. Without an effective e-mail system, the company will operate with less efficiency. A number of organizations have suffered failure of their e-mail systems as a result of mass e-mailed worms in past years. New exploits transferred using e-mail are reported. Those exploiting vulnerabilities in common applications are of major concern. The heavy use of e-mail by the company, including the constant exchange and opening of e-mail attachments by employees, means the chance of compromise, especially by a zero-day exploit to a common document type, is very high. While the company does filter mail in its Internet gateway, there is a high probability that a zero-day exploit would not be caught. A denial of service attack against the mail gateway is very hard to defend against. Hence a likelihood rating of Almost Certain was selected in recognition of the wide range of possible attacks and the high chance that one will occur sooner rather than later. Discussions with management indicated that while other possible modes of communication exist, they do not allow for transmission of electronic documents. The ability to obtain electronic quotes is a requirement that must be met to place an order in the purchasing system. Reports and other communications are regularly sent via this e-mail, and any inability to send or receive such reports might affect the company's reputation. There would also be financial costs and time needed to rebuild the e-mail system following a serious compromise. Because compromise would not have a large impact, a consequence rating of Minor was selected. This results in a risk level of High.

The information was summarized and presented to management. All of the resulting risk levels are above the acceptable minimum management specified as tolerable. Hence treatment is required. Even though the second asset listed had the

highest level of risk, management decided that the risk to the SCADA network was unacceptable if there was any possibility of death, however remote. Additionally, the management decided that the government regulator would not look favorably upon a company that failed to rate highly the importance of a potential fatality. Consequently, the management decided to specify the risk to the SCADA as the highest priority for treatment. The risk to the integrity of stored information was next. The management also decided to place the risk to the e-mail systems last, behind the lower risk to the Maintenance/Production system, in part because its compromise would not affect the output of the mining and processing units and also because treatment would involve the company's mail gateway, which was outside the management's control.

The final result of this risk assessment process is shown in Table 14.6, the resulting overall risk register table. It shows the identified assets with the threats to them, and the assigned ratings and priority. This information would then influence the selection of suitable treatments. Management decided the first five risks should be treated by implementing suitable controls, which would reduce either the likelihood or the consequence should these risks occur. This process is discussed in the next chapter. None of these risks could be accepted or avoided. Responsibility for the final risk to the e-mail system was found to be primarily with the parent company's IT group, which manages the external mail gateway. Hence the risk is shared with that group.

14.6 Recommended Reading

[SLAY06] provides a discussion of issues involved with IT security management. [SCHN00] provides a very readable, general discussion of IT security issues and myths in the modern world. Current best practice in the field of IT security management is codified in a range of international and national standards, whose use is encouraged. These standards include [ISO27001], [ISO27002], [ISO27005], [ISO31000], [NIST95], [NIST09], [NIST12], [NIST13], [SASN06], and [SA04].

ISO13335 ISO/IEC, "ISO/IEC 13335-1:2004—Information technology—Security techniques—Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management," 2004.

ISO27001 ISO/IEC, "ISO/IEC 27001:2005—Information technology—Security techniques—Information security management systems—Requirements," 2005.

ISO27002 ISO/IEC, "ISO/IEC 27002:2005—Information technology—Security techniques—Code of practice for information security management," 2005. Formerly known as ISO/IEC 17755:2005.

ISO27005 ISO/IEC, "ISO/IEC 27005:2011—Information technology—Security techniques—Information security risk management," 2011.

ISO31000 ISO, "ISO 31000:2009—Risk management—Principles and guidelines," 2009.

NIST95 National Institute of Standards and Technology, *An Introduction to Computer Security: The NIST Handbook*, Special Publication 800-12, October 1995.

NIST09 National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems,* Special Publication 800-53 Revision 3, August 2009.

NIST12 National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, Special Publication 800-30 Revision 1, September 2012.

NIST13 National Institute of Standards and Technology, *Guide to Industrial Control Systems (ICS) Security,* Special Publication 800-82 Revision 1, April 2013.

SA04 Standards Australia, "HB 231:2004—Information Security Risk Management Guidelines," 2004.

SASN06 Standards Australia and Standards New Zealand, "HB 167:2006—Security Risk Management," 2006.

SCHN00 Schneier, B. *Secrets & Lies—Digital Security in a Networked World*, New York: John Wiley & Sons, 2000.

SLAY06 Slay, J., and Koronios, A. *Information Technology Security & Risk Management*. Milton, QLD: John Wiley & Sons Australia, 2006.

14.7 key Ter MS, r ev Iew Qu eSTIOn S, a n d Pr Ob l eMS

Key Terms

asset	likelihood	risk register
consequence	organizational security policy	threat
control	risk	threat source
IT security management	risk appetite	vulnerability
level of risk	risk assessment	

Review Questions

14.1 Define *IT security management*.

14.2 List the three fundamental questions IT security management tries to address.

14.3 List the steps in the process used to address the three fundamental questions.

14.4 List some of the key national and international standards that provide guidance on IT security management and risk assessment.

14.5 List and briefly define the four steps in the iterative security management process.

14.6 Organizational security objectives identify what IT security outcomes are desired, based in part on the role and importance of the IT systems in the organization. List some questions that help clarify these issues.

14.7 List and briefly define the four approaches to identifying and mitigating IT risks.

14.8 Which of the four approaches for identifying and mitigating IT risks does [ISO13335] suggest is the most cost effective for most organizations?

14.9 List the steps in the detailed security risk analysis process.

14.10 Define *asset*, *control, threat, risk,* and *vulnerability*.

14.11 Indicate who provides the key information when determining each of the key assets, their likelihood of compromise, and the consequence should any be compromised.

14.12 State the two key questions answered to help identify threats and risks for an asset. Briefly indicate how these questions are answered.

14.13 Define *consequence* and *likelihood*.

14.14 What is the simple equation for determining risk? Why is this equation not commonly used in practice?

14.15 What are the items specified in the risk register for each asset/threat identified?

14.16 List and briefly define the five alternatives for treating identified risks.

Problems

14.1 Research the IT security policy used by your university or by some other organization you are associated with. Identify which of the topics listed in Section 14.2 this policy addresses. If possible, identify any legal or regulatory requirements that apply to the organization. Do you believe the policy appropriately addresses all relevant issues? Are there any topics the policy should address but does not?

14.2 As part of a formal risk assessment of desktop systems in a small accounting firm with limited IT support, you have identified the asset "integrity of customer and financial data files on desktop systems" and the threat "corruption of these files due to import of a worm/virus onto system." Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.

14.3 As part of a formal risk assessment of the main file server for a small legal firm, you have identified the asset "integrity of the accounting records on the server" and the threat "financial fraud by an employee, disguised by altering the accounting records." Suggest reasonable values for the items in the risk register for this asset and threat with justifications for your choice.

14.4 As part of a formal risk assessment of the external server in a small Web design company, you have identified the asset "integrity of the organization's Web server" and the threat "hacking and defacement of the Web server." Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.

14.5 As part of a formal risk assessment of the main file server in an IT security consultancy firm, you have identified the asset "confidentiality of techniques used to conduct penetration tests on customers, and the results of conducting such tests for clients, which are stored on the server" and the threat "theft/breach of this confidential and sensitive information by either an external or internal source." Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.

14.6 As part of a formal risk assessment on the use of laptops by employees of a large government department, you have identified the asset "confidentiality of personnel information in a copy of a database stored unencrypted on the laptop" and the threat "theft of personal information, and its subsequent use in identity theft caused by the theft of the laptop." Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.

14.7 As part of a formal risk assessment process for a small public service agency, suggest some threats that such an agency is exposed to. Use the checklists, provided in the various risk assessment standards cited in this chapter, to assist you.

14.8 A copy of the original version of NIST SP 800-30 from 2002 is available at box.com/CompSec3e. Compare Tables 3.4 to 3.7 from that document which specify levels of likelihood, consequence, and risk, with our equivalent Tables 14.2–14.4 in this chapter. What are the key differences? What is the effect on the level of detail in risk assessments using these alternate tables? Why do you think the NIST tables were changed significantly in the latest version?

CHAPTER 15

IT Security Controls, Plans, and Procedures

LEARNING OBJECTIVES

After studying this chapter, you should be able to:

- List the various categories and types of controls available.
- Outline the process of selecting suitable controls to address risks.
- Outline an implementation plan to address identified risks.
- Understand the need for ongoing security implementation follow-up.

In Chapter 14, we introduced IT security management as a formal process to ensure that critical assets are sufficiently protected in a cost-effective manner. We then discussed the critical risk assessment process. This chapter continues the examination of IT security management. We survey the range of management, operational, and technical controls or safeguards available that can be used to improve security of IT systems and processes. We then explore the content of the security plans that detail the implementation process. These plans must then be implemented, with training to ensure that all personnel know their responsibilities, and monitoring to ensure compliance. Finally, to ensure that a suitable level of security is maintained, management must follow up the implementation with an evaluation of the effectiveness of the security controls and an iteration of the entire IT security management process.

15.1 IT Security Management Implementation

We introduced the IT security management process in Chapter 14, illustrated by Figure 14.1. Chapter 14 focused on the earlier stages of this process. In this chapter we focus on the latter stages, which include selecting controls, developing an implementation plan, and the follow-up monitoring of the plan's implementation. We broadly follow the guidance provided in [NIST11], which was developed by NIST as the flagship document for providing guidance for an integrated, organization-wide program for managing information security risk, in response to FISMA. A broad summary of these steps is given in Figure 15.1. We discuss each of these in turn.

15.2 Security Controls or Safeguards

A risk assessment on an organization's IT systems identifies areas needing treatment. The next step, as shown in Figure 14.1 on risk analysis options, is to select suitable controls to use in this treatment. An IT security **control**, **safeguard**, or **countermeasure** (the terms are used interchangeably) helps to reduce risks. We use the following definition:

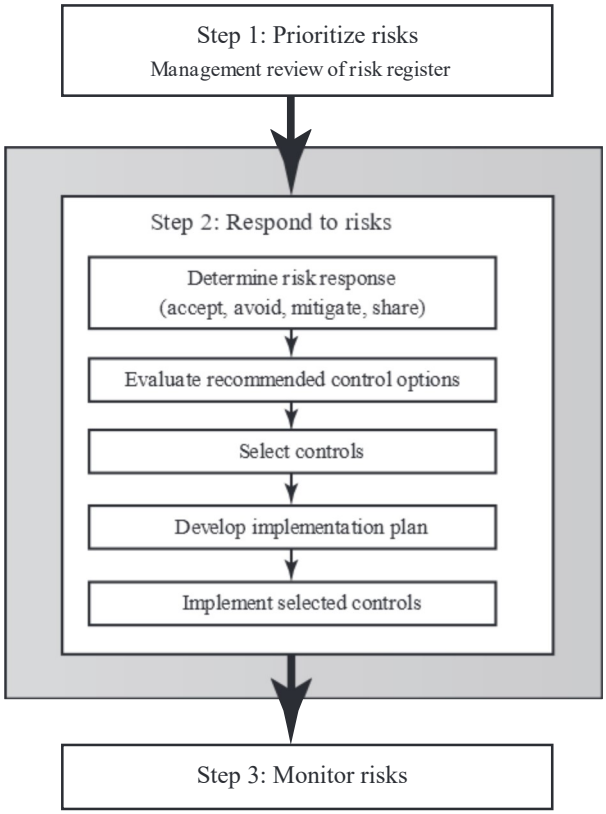

Figure 15.1 **IT Security Management Controls and Implementation**

control: An action, device, procedure, or other measure that reduces risk by eliminating or preventing a security violation, by minimizing the harm it can cause, or by discovering and reporting it to enable corrective action.

Some controls address multiple risks at the same time, and selecting such controls can be very cost effective. Controls can be classified as belonging to one of the following classes (although some controls include features from several of these):

- **Management controls:** Focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission. These controls refer to issues that management needs to address. We discuss a number of these in Chapters 14 and 15.
- **Operational controls:** Address the correct implementation and use of security policies and standards, ensuring consistency in security operations and correcting identified operational deficiencies. These controls relate to mechanisms and procedures that are primarily implemented by people rather

than systems. They are used to improve the security of a system or group of systems. We discuss some of these in Chapters 16 and 17.

- **Technical controls:** Involve the correct use of hardware and software security capabilities in systems. These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions. Figure 15.2 illustrates some typical technical control measures. Parts One and Two in this text discuss aspects of such measures.

In turn, each of these control classes may include the following:

- **Supportive controls:** Pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls.
- **Preventative controls:** Focus on preventing security breaches from occurring, by inhibiting attempts to violate security policies or exploit a vulnerability.
- **Detection and recovery controls:** Focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability and by providing means to restore the resulting lost computing resources.

The technical control measures shown in Figure 15.2 include examples of each of these types of controls.

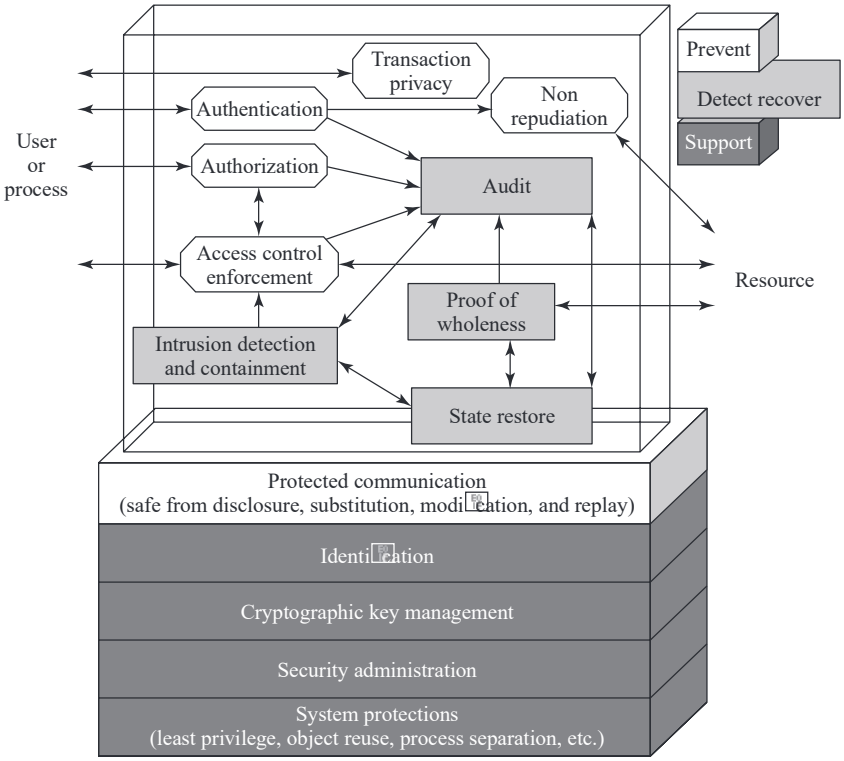

Figure 15.2 Technical Security Controls

Lists of controls are provided in a number of national and international standards, including [ISO27002], [ISO13335], and [NIST09]. There is broad agreement among these and other standards as to the types of controls that should be used and the detailed lists of typical controls. Indeed many of the standards cross-reference each other, indicating their agreement on these lists. [ISO27002] is generally regarded as the master list of controls and is cited by most other standards. Table 15.1 (adapted from Table 1-1 in [NIST09]) is a typical list of families of controls within each of the classes. Compare this with the list in Table 15.2, which details the categories of controls given in [ISO27002], noting the high degree of overlap. Within each of these control classes, there is a long list of specific controls that may be chosen. Table 15.3 (adapted from the table in Appendix D of [NIST09]) itemizes the full list of controls detailed in this standard.

To attain an acceptable level of security, some combination of these controls should be chosen. If the baseline approach is being used, an appropriate baseline set of controls is typically specified in a relevant industry or government standard. For example, Appendix D in [NIST09] lists selections of baseline controls for use in low-, moderate-, and high-impact IT systems. A selection should be made that is appropriate to the organization's overall risk profile, resources, and capabilities. These should then be implemented across all the IT systems for the organization, with adjustments in scope to address broad requirements of specific systems.

Table 15.1 NIST SP800-53 Security Controls

Class	Control Family
Management	Planning
Management	Program Management
Management	Risk Assessment
Management	Security Assessment and Authorization
Management	System and Services Acquisition
Operational	Awareness and Training
Operational	Configuration Management
Operational	Contingency Planning
Operational	Incident Response
Operational	Maintenance
Operational	Media Protection
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	System and Information Integrity
Technical	Access Control
Technical	Audit and Accountability
Technical	Identification and Authentication
Technical	System and Communications Protection

Table 15.2 ISO/IEC 27002 Security Controls

Control Category	Objective
Security Policies	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
Organization of Information Security	To establish a management framework to initiate and control the implementation and operation of information security within the organization, and to ensure the security of teleworking and use of mobile devices.
Human Resource Security	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered, and to ensure that employees and contractors are aware of and fulfill their information security responsibilities, and to protect the organization's interests as part of the process of changing or terminating employment.
Asset Management	To identify organizational assets and define appropriate protection responsibilities, and to ensure that information receives an appropriate level of protection in accordance with its importance to the organization, and to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.
Access Control	To limit access to information and information processing facilities, and to ensure authorized user access and to prevent unauthorized access to systems and services, and to make users accountable for safeguarding their authentication information, and to prevent unauthorized access to systems and applications.
Cryptography	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Physical and Environmental Security	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities; to prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Operations Security	To ensure correct and secure operations of information processing facilities; to ensure that information and information processing facilities are protected against malware; to protect against loss of data; to record events and generate evidence; to ensure the integrity of operational systems to prevent exploitation of technical vulnerabilities.
Communications Security	To ensure the protection of information in networks and its supporting information processing facilities; maintain the security of information transferred within an organization and with an external entity.
System Acquisition, Development and Maintenance	To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks; ensure that information security is designed and implemented within the development lifecycle of information systems; ensure the protection of data used for testing.
Supplier Relationships	To maintain an agreed level of information security and service delivery in line with supplier agreements.
Information Security Incident Management	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
Information Security Continuity	To embed in the organization's business continuity management systems; ensure availability of information processing facilities.
Compliance	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements; ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

Table 15.3 Detailed NIST SP800-53 Security Controls

Access Control Access Control Policy and Procedures, Account Management, Access Enforcement, Information Flow Enforcement, Separation of Duties, Least Privilege, Unsuccessful Login Attempts, System Use Notification, Previous Logon (Access) Notification, Concurrent Session Control, Session Lock, Permitted Actions without Identification or Authentication, Security Attributes, Remote Access, Wireless Access, Access Control for Mobile Devices, Use of External Information Systems, User-Based Collaboration and Information Sharing, Publicly Accessible Content
Awareness and Training Security Awareness and Training Policy and Procedures, Security Awareness, Security Training, Security Training Records, Contacts with Security Groups and Associations
Audit and Accountability Audit and Accountability Policy and Procedures, Auditable Events, Content of Audit Records, Audit Storage Capacity, Response to Audit Processing Failures, Audit Review, Analysis, and Reporting, Audit Reduction and Report Generation, Time Stamps, Protection of Audit Information, Nonrepudiation, Audit Record Retention, Audit Generation, Monitoring for Information Disclosure, Session Audit
Security Assessment and Authorization Security Assessment and Authorization Policies and Procedures, Security Assessments, Information System Connections, Plan of Action and Milestones, Security Accreditation, Continuous Monitoring
Configuration Management Configuration Management Policy and Procedures, Baseline Configuration, Configuration Change Control, Security Impact Analysis, Access Restrictions for Change, Configuration Settings, Least Functionality, Information System Component Inventory, Configuration Management Plan
Contingency Planning Contingency Planning Policy and Procedures, Contingency Plan, Contingency Training, Contingency Plan Testing and Exercises, Alternate Storage Site, Alternate Processing Site, Telecommunications Services, Information System Backup, Information System Recovery and Reconstitution
Identification and Authentication Identification and Authentication Policy and Procedures, Identification and Authentication (Organizational Users), Device Identification and Authentication, Identifier Management, Authenticator Management, Authenticator Feedback, Cryptographic Module Authentication, Identification and Authentication (Nonorganizational Users)
Incident Response Incident Response Policy and Procedures, Incident Response Training, Incident Response Testing and Exercises, Incident Handling, Incident Monitoring, Incident Reporting, Incident Response Assistance, Incident Response Plan
Maintenance System Maintenance Policy and Procedures, Controlled Maintenance, Maintenance Tools, Nonlocal Maintenance, Maintenance Personnel, Timely Maintenance
Media Protection Media Protection Policy and Procedures, Media Access, Media Marking, Media Storage, Media Transport, Media Sanitization
Physical and Environmental Protection Physical and Environmental Protection Policy and Procedures, Physical Access Authorizations, Physical Access Control, Access Control for Transmission Medium, Access Control for Output Devices, Monitoring Physical Access, Visitor Control, Access Records, Power Equipment and Power Cabling, Emergency Shutoff, Emergency Power, Emergency Lighting, Fire Protection, Temperature and Humidity Controls, Water Damage Protection, Delivery and Removal, Alternate Work Site, Location of Information System Components, Information Leakage

(Continued)

Table 15.3 (Continued)

Planning Security Planning Policy and Procedures, System Security Plan, Rules of Behavior, Privacy Impact Assessment, Security-Related Activity Planning
Personnel Security Personnel Security Policy and Procedures, Position Categorization, Personnel Screening, Personnel Termination, Personnel Transfer, Access Agreements, Third-Party Personnel Security, Personnel Sanctions
Risk Assessment Risk Assessment Policy and Procedures, Security Categorization, Risk Assessment, Vulnerability Scanning
System and Services Acquisition System and Services Acquisition Policy and Procedures, Allocation of Resources, Life Cycle Support, Acquisitions, Information System Documentation, Software Usage Restrictions, User Installed Software, Security Engineering Principles, External Information System Services, Developer Configuration Management, Developer Security Testing, Supply Chain Protection, Trustworthiness, Critical Information System Components
System and Communications Protection System and Communications Protection Policy and Procedures, Application Partitioning, Security Function Isolation, Information in Shared Resources, Denial of Service Protection, Resource Priority, Boundary Protection, Transmission Integrity, Transmission Confidentiality, Network Disconnect, Trusted Path, Cryptographic Key Establishment and Management, Use of Cryptography, Public Access Protections, Collaborative Computing Devices, Transmission of Security Attributes, Public Key Infrastructure Certificates, Mobile Code, Voice Over Internet Protocol, Secure Name/Address Resolution Service (Recursive or Caching Resolver), Architecture and Provisioning for Name/Address Resolution Service, Session Authenticity, Fail in Known State, Thin Nodes, Honeypots, Operating System-Independent Applications, Protection of Information at Rest, Heterogeneity, Virtualization Techniques, Covert Channel Analysis, Information System Partitioning, Transmission Preparation Integrity, Nonmodifiable Executable Programs
System and Information Integrity System and Information Integrity Policy and Procedures, Flaw Remediation, Malicious Code Protection, Information System Monitoring, Security Alerts Advisories and Directives, Security Functionality Verification, Software and Information Integrity, Spam Protection, Information Input Restrictions, Information Input Validation, Error Handling, Information Output Handling and Retention, Predictable Failure Prevention
Program Management Information Security Program Plan, Senior Information Security Officer, Information Security Resources, Plan of Action and Milestones Process, Information System Inventory, Information Security Measures of Performance, Enterprise Architecture, Critical Infrastructure Plan, Risk Management Strategy, Security Authorization Process, Mission/Business Process Definition

[NIST06] suggests that adjustments may be needed for considerations related to the following:

- **Technology:** Some controls are only applicable to specific technologies, and hence these controls are only needed if the system includes those technologies. Examples of these include wireless networks and the use of cryptography. Some may only be appropriate if the system supports the technology they require—for example, readers for access tokens. If these technologies are not supported on a system, then alternate controls, including administrative procedures or physical access controls, may be used instead.
- **Common controls:** The entire organization may be managed centrally and may not be the responsibility of the managers of a specific system. Control changes would need to be agreed to and managed centrally.

- **Public access systems:** Some systems, such as the organization's public Web server, are designed for access by the general public. Some controls, such as those relating to personnel security, identification, and authentication, would not apply to access via the public interface. They would apply to administrative control of such systems. The scope of application of such controls must be specified carefully.
- **Infrastructure controls:** Physical access or environmental controls are only relevant to areas housing the relevant equipment.
- **Scalability issues:** Controls may vary in size and complexity in relation to the organization employing them. For example, a contingency plan for systems critical to a large organization would be much larger and more detailed than that for a small business.
- **Risk assessment:** Controls may be adjusted according to the results of specific risk assessment of systems in the organization, as we now consider.

If some form of informal or formal risk assessment process is being used, then it provides guidance on specific risks to an organization's IT systems that need to be addressed. These will typically be some selection of operational or technical controls that together can reduce the likelihood of the identified risk occurring, the consequences if it does, or both, to an acceptable level. These may be in addition to those controls already selected in the baseline, or may simply be more detailed and careful specification and use of already selected controls.

The process illustrated in Figure 15.1 indicates that a recommended list of controls should be made to address each risk needing treatment. The recommended controls need to be compatible with the organization's systems and policies, and their selection may also be guided by legal requirements. The resulting list of controls should include details of the feasibility and effectiveness of each control. The feasibility addresses factors such as technical compatibility with and operational impact on existing systems and user's likely acceptance of the control. The effectiveness equates the cost of implementation against the reduction in level of risk achieved by implementing the control.

The reduction in level of risk that results from implementing a new or enhanced control results from the reduction in threat likelihood or consequence that the control provides, as shown in Figure 15.3. The reduction in likelihood may result either by reducing the vulnerabilities (flaws or weaknesses) in the system or by reducing the capability and motivation of the threat source. The reduction in consequence occurs by reducing the magnitude of the adverse impact of the threat occurring in the organization.

It is likely that the organization will not have the resources to implement all the recommended controls. Therefore, management should conduct a cost-benefit analysis to identify those controls that are most appropriate, and provide the greatest benefit to the organization given the available resources. This analysis may be qualitative or quantitative and must demonstrate that the cost of implementing a given control is justified by the reduction in level of risk to assets that it provides. It should include details of the impact of implementing the new or enhanced control, the impact of not implementing it, and the estimated costs of implementation.

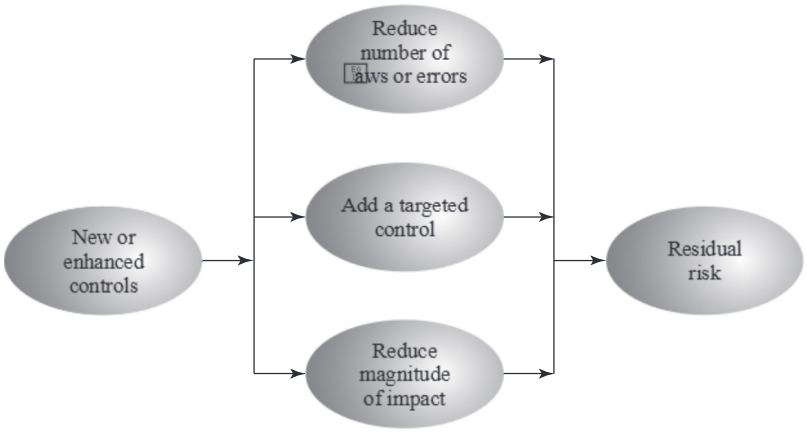

Figure 15.3 **Residual Risk**

It must then assess the implementation costs and benefits against system and data criticality to determine the importance of choosing this control.

Management must then determine which selection of controls provides an acceptable resulting level of risk to the organization's systems. This selection will consider factors such as the following:

- If the control would reduce risk more than needed, then a less expensive alternative could be used.
- If the control would cost more than the risk reduction provided, then an alternative should be used.
- If a control does not reduce the risk sufficiently, then either more or different controls should be used.
- If the control provides sufficient risk reduction and is the most cost effective, then use it.

It is often the case that the cost of implementing a control is more tangible and easily specified than the cost of not implementing it. Management must make a business decision regarding these ill-defined costs in choosing the final selection of controls and resulting residual risk.

15.3 IT Security Plan

Having identified a range of possible controls from which management has selected some to implement, an IT security plan should then be created, as indicated in Figures 14.1 and 15.1. This is a document that provides details as to what will be done, what resources are needed, and who will be responsible. The goal is to detail the actions needed to improve the identified deficiencies in the organization's risk profile in a timely manner. [NIST12] suggests that this plan should include details of

- Risks (asset/threat/vulnerability combinations)
- Recommended controls (from the risk assessment)

Table 15.4 Implementation Plan

Risk (Asset/Threat)	Hacker attack on Internet router
Level of Risk	High
Recommended Controls	• Disable external telnet access • Use detailed auditing of privileged command use • Set policy for strong admin passwords • Set backup strategy for router configuration file • Set change control policy for the router configuration
Priority	High
Selected Controls	• Strengthen access authentication • Install intrusion detection software
Required Resources	• 3 days IT net admin time to change and verify router configuration, write policies • 1 day of training for network administration staff
Responsible Persons	John Doe, Lead Network System Administrator, Corporate IT Support Team
Start to End Date	February 1, 2011 to February 4, 2011
Other Comments	• Need periodic test and review of configuration and policy use

- Action priority for each risk
- Selected controls (on the basis of the cost-benefit analysis)
- Required resources for implementing the selected controls
- Responsible personnel
- Target start and end dates for implementation
- Maintenance requirements and other comments

These details are summarized in an **implementation plan** table, such as that shown in Table 15.4. This illustrates an example implementation plan for the example risk identified and shown in Table 14.5. The suggested controls are specific examples of remote access, auditable event, user identification, system backup, and configuration change controls, applied to the identified threatened asset. All of them are chosen, because they are neither costly nor difficult to implement. They do require some changes to procedures. The relevant network administration staff must be notified of these changes. Staff members may also require training on the correct implementation of the new procedures and their rights and responsibilities.

15.4 Implementation of controls

The next phase in the IT security management process, as indicated in Figure 14.1, is to manage the implementation of the controls detailed in the IT security plan. This comprises the *do* stage of the cyclic implementation model discussed in Chapter 14. The implementation phase comprises not only the direct implementation of the controls as detailed in the security plan, but also the associated specific training and general security awareness programs for the organization.

Implementation of Security Plan

The **IT security plan** documents what needs to be done for each selected control, along with the personnel responsible, and the resources and time frame to be used. The identified personnel then undertake the tasks needed to implement the new or enhanced controls, be they technical, managerial, or operational. This may involve some combination of system configuration changes, upgrades, or new system installation. It may also involve the development of new or extended procedures to document practices needed to achieve the desired security goals. Note that even technical controls typically require associated operational procedures to ensure their correct use. The use of these procedures needs to be encouraged and monitored by management.

The implementation process should be monitored to ensure its correctness. This is typically performed by the organizational security officer, who checks that:

- The implementation costs and resources used stay within identified bounds.
- The controls are correctly implemented as specified in the plan, in order that the identified reduction in risk level is achieved.
- The controls are operated and administered as needed.

When the implementation is successfully completed, management needs to authorize the system for operational use. This may be a purely informal process within the organization. Alternatively, especially in government organizations, this may be part of a formal process resulting in accreditation of the system as meeting required standards. This is usually associated with the installation, certification, and use of trusted computing system, as we discuss in Chapter 13. In these cases an external accrediting body will verify the documented evidence of the correct design and implementation of the system.

Security Awareness and Training

Appropriate security awareness training for all personnel in an organization, along with specific training relating to particular systems and controls, is an essential component in implementing controls. We discuss these issues further in Chapter 17, where we explore policies related to personnel security.

15.5 Monitoring Risks

The IT security management process does not end with the implementation of controls and the training of personnel. As we noted in Chapter 14, it is a cyclic process, constantly repeated to respond to changes in the IT systems and the risk environment. The various controls implemented should be monitored to ensure their continued effectiveness. Any proposed changes to systems should be checked for security implications and the risk profile of the affected system reviewed if necessary. Unfortunately, this aspect of IT security management often receives the least attention and in many cases is added as an afterthought, if at all. Failure

to do so can greatly increase the likelihood that a security failure will occur. This follow-up stage of the management process includes a number of aspects:

- Maintenance of security controls
- Security compliance checking
- Change and configuration management
- Incident handling

Any of these aspects might indicate that changes are needed to the previous stages in the IT security management process. An obvious example is that if a breach should occur, such as a virus infection of desktop systems, then changes may be needed to the risk assessment, to the controls chosen, or to the details of their implementation. This can trigger a review of earlier stages in the process.

Maintenance

The first aspect concerns the continued maintenance and monitoring of the implemented controls to ensure their continued correct functioning and appropriateness. It is important that someone has responsibility for this maintenance process, which is generally coordinated by the organization's security officer. The maintenance tasks include ensuring that:

- Controls are periodically reviewed to verify that they still function as intended.
- Controls are upgraded when new requirements are discovered.
- Changes to systems do not adversely affect the controls.
- New threats or vulnerabilities have not become known.

This review includes regular analysis of log files to ensure various system components are functioning as expected, and to determine a baseline of activity against which abnormal events can be compared when handling incidents. We discuss security auditing further in Chapter 18.

The goal of maintenance is to ensure that the controls continue to perform as intended, and hence that the organization's risk exposure remains as chosen. Failure to maintain controls could lead to a security breach with a potentially significant impact on the organization.

Security Compliance

Security compliance checking is an audit process to review the organization's security processes. The goal is to verify compliance with the security plan. The audit may be conducted using either internal or external personnel. It is generally based on the use of checklists, which verify that the suitable policies and plans have been created, that suitable controls were chosen, and that the controls are maintained and used correctly.

This audit process should be conducted on new IT systems and services once they are implemented; and on existing systems periodically, often as part of a wider, general audit of the organization or whenever changes are made to the organization's security policy.

Change and Configuration Management

Change management is the process used to review proposed changes to systems for implications on the organization's systems and use. Changes to existing systems can occur for a number of reasons, such as the following:

- Users reporting problems or desired enhancements
- Identification of new threats or vulnerabilities
- Vendor notification of patches or upgrades to hardware or software
- Technology advances
- Implementation of new IT features or services, which require changing existing systems
- Identification of new tasks, which require changing existing systems

The impact of any proposed change on the organization's systems should be evaluated. This includes not only security-related aspects, but wider operational issues as well. Thus change management is an important component of the general systems administration process. Because changes can affect security, this general process overlaps IT security management and must interact with it.

An important example is the constant flow of patches addressing bugs and security failings in common operating systems and applications. If the organization is running systems of any complexity, with a range of applications, then patches should ideally be tested to ensure that they don't adversely affect other applications. This can be a time-consuming process that may require considerable administration resources. If patch testing is not done, one alternative is to delay patching or upgrading systems. This could leave the organization exposed to a new vulnerability for a period. Otherwise the patches or upgrades could be applied without testing, which may result in other failures in the systems and the loss of functionality.

Ideally, most proposed changes should act to improve the security profile of a system. However, it is possible that for imperative business reasons a change is proposed that reduces the security of a system. In cases like this, it is important that the reasons for the change, its consequences on the security profile for the organization, and management authorization of it be documented. The benefits to the organization would need to be traded off against the increased risk level.

The change management process may be informal or formal, depending on the size of the organization and its overall IT management processes. In a formal process, any proposed change should be documented and tested before implementation. As part of this process, any related documentation, including relevant security documentation and procedures, should be updated to reflect the change.

Configuration management is concerned with specifically keeping track of the configuration of each system in use and the changes made to each. This includes lists of the hardware and software versions installed on each system. This information is needed to help restore systems following a failure (whether security related or not) and to know what patches or upgrades might be relevant to particular systems. Again, this is a general systems administration process with security implications and must interact with IT security management.

Incident Handling

The procedures used to respond to a security incident comprise the final aspect included in the follow-up stage of IT security management. This topic is discussed further in Chapter 17, where we explore policies related to human factors.

15.6 Case Study: Silver Star Mines

Consider the case study introduced in Chapter 14, which involves the operations of a fictional company Silver Star Mines. Given the outcome of the risk assessment for this company, the next stage in the security management process is to identify possible controls. From the information provided during this assessment, clearly a number of the possible controls listed in Table 15.3 are not being used. A comment repeated many times was that many of the systems in use had not been regularly upgraded, and part of the reason for the identified risks was the potential for system compromise using a known but unpatched vulnerability. That clearly suggests that attention needs to be given to controls relating to the regular, systematic maintenance of operating systems and applications software on server and client systems. Such controls include:

- Configuration management policy and procedures
- Baseline configuration
- System maintenance policy and procedures
- Periodic maintenance
- Flaw remediation
- Malicious code protection
- Spam and spyware protection

Given that potential incidents are possible, attention should also be given to developing contingency plans to detect and respond to such incidents and to enable speedy restoration of system function. Attention should be paid to controls such as:

- Audit monitoring, analysis, and reporting
- Audit reduction and report generation
- Contingency planning policy and procedures
- Incident response policy and procedures
- Information system backup
- Information system recovery and reconstitution

These controls are generally applicable to all the identified risks and constitute good general systems administration practice. Hence, their cost effectiveness would be high because they provide an improved level of security across multiple identified risks.

Now consider the specific risk items. The top-priority risk relates to the reliability and integrity of the Supervisory Control and Data Acquisition (SCADA) nodes and network. These were identified as being at risk because many of these systems are running older releases of operating systems with known insecurities. Further, these systems cannot be patched or upgraded because the key applications they run have not been updated or validated to run on newer OS versions. Given these limitations on the ability to reduce the vulnerability of individual nodes, attention should be paid to the firewall and application proxy servers that isolate the SCADA nodes and network from the wider corporate network. These systems can be regularly maintained and managed according to the generally applied list of controls we identified. Further, because the traffic to and from the SCADA network is highly structured and predictable, it should be possible to implement an intrusion detection system with much greater reliability than applies to general-use corporate networks. This system should be able to identify attack traffic, as it would be very different from normal traffic flows. Such a system might involve a more detailed, automated analysis of the audit records generated on the existing firewall and proxy server systems. More likely, it could be an independent system connected to and monitoring the traffic through these systems. The system could be further extended to include an automated response capability, which could automatically sever the network connection if an attack is identified. This approach recognizes that the network connection is not needed for the correct operation of the SCADA nodes. Indeed, they were designed to operate without such a network connection, which is much of the reason for their insecurity. All that would be lost is the improved overall monitoring and management of the SCADA nodes. With this functionality, the likelihood of a successful attack, already regarded as very unlikely, can be further reduced.

The second priority risk relates to the integrity of stored information. Clearly all the general controls help ameliorate this risk. More specifically, much of the problem relates to the large number of documents scattered over a large number of systems with inconsistent management. This risk would be easier to manage if all documents identified as critical to the operation of the company were stored on a smaller pool of application and file servers. These could be managed appropriately using the generally applicable controls. This suggests that an audit of critical documents is needed to identify who is responsible for them and where they are currently located. Then policies are needed that specify that critical documents should be created and stored only on approved central servers. Existing documents should be transferred to these servers. Appropriate education and training of all affected users is needed to help ensure that these policies are followed.

The next three risks relate to the availability or integrity of the key Financial, Procurement, and Maintenance/Production systems. The generally applicable controls we identified should adequately address these risks once the controls are applied to all relevant servers.

The final risk relates to the availability, integrity, and confidentiality of e-mail. As was noted in the risk assessment, this is primarily the responsibility of the parent company's IT group that manages the external mail gateway. There is a limited amount that can be done on the local site. The use of the generally applicable

controls, particularly those relating to malicious code protection and spam and spyware protection on client systems, will assist in reducing this risk. In addition, as part of the contingency planning and incident response policies and procedures, consideration could be given to a backup e-mail system. For security this system would use client systems isolated from the company intranet, connected to an external local network service provider. This connection would be used to provide limited e-mail capabilities for critical messages should the main company intranet e-mail system be compromised.

This analysis of possible controls is summarized in Table 15.5, which lists the controls identified and the priorities for their implementation. This table must be extended to include details of the resources required, responsible personnel, time frame, and any other comments. This plan would then be implemented, with suitable monitoring of its progress. Its successful implementation leads then to longer term follow-up, which should ensure that the new policies continue to be applied appropriately and that regular reviews of the company's security profile occur. In time this should lead to a new cycle of risk assessment, plan development, and follow-up.

Table 15.5 Silver Star Mines—Implementation Plan

Risk (Asset/Threat)	Level of Risk	Recommended Controls	Priority	Selected Controls
All risks (generally applicable)		1. Configuration and periodic maintenance policy for servers 2. Malicious code (SPAM, spyware) prevention 3. Audit monitoring, analysis, reduction, and reporting on servers 4. Contingency planning and incident response policies and procedures 5. System backup and recovery procedures	1	1. 2. 3. 4. 5.
Reliability and integrity of SCADA nodes and network	High	1. Intrusion detection and response system	2	1.
Integrity of stored file and database information	Extreme	1. Audit of critical documents 2. Document creation and storage policy 3. User security education and training	3	1. 2. 3.
Availability and integrity of Financial, Procurement, and Maintenance/ Production Systems	High	—	—	(general controls)
Availability, integrity, and confidentiality of e-mail	High	1. Contingency planning—backup e-mail service	4	1.

15.7 Recommended Reading

More general discussion of the issues involved with IT security management is found in [MAIW02] and [SLAY06]. Current best practice in the field of IT security management is codified in a range of international and national standards, whose use is encouraged. These standards include [ISO13335], [ISO27001], [ISO27002], [ISO27005], [NIST06], [NIST09], [NIST11], and [NIST12].

ISO13335 ISO/IEC, "ISO/IEC 13335-1:2004—Information technology—Security techniques—Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management," 2004.

ISO27001 ISO/IEC, "ISO/IEC 27001:2005—Information technology—Security techniques—Information security management systems—Requirements," 2005.

ISO27002 ISO/IEC, "ISO/IEC 27002:2005—Information technology—Security techniques—Code of practice for information security management," 2005. Formerly known as ISO/IEC 17755:2005.

ISO27005 ISO/IEC, "ISO/IEC 27005:2011—Information technology—Security techniques—Information security risk management," 2011.

MAIW02 Maiwald, E., and Sieglein, W. *Security Planning & Disaster Recovery*, Berkeley, CA: McGraw-Hill/Osborne, 2002.

NIST06 National Institute of Standards and Technology. *Guide for Developing Security Plans for Federal Information Systems*. Special Publication 800-18 Revision 1, February 2006.

NIST09 National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems*. Special Publication 800-53 Revision 3, August 2009.

NIST11 National Institute of Standards and Technology. *Managing Information Security Risk: Organization, Mission, and Information System View*. Special Publication 800-39, March 2011.

NIST12 National Institute of Standards and Technology. *Risk Management Guide for Information Technology Systems*. Special Publication 800-30 Revision 1, September 2012.

SLAY06 Slay, J., and Koronios, A. *Information Technology Security & Risk Management*, Milton, QLD: John Wiley & Sons Australia, 2006.

15.8 Key Terms, Review Questions, and Problems

Key Terms

change management	implementation plan	safeguard
configuration management	IT security plan	security compliance
control	management control	supportive control
countermeasure	operational control	technical control
detection and recovery control	preventative control	

Review Questions

15.1 Define *security control* or *safeguard*.

15.2 List and briefly define the three broad classes of controls and the three categories each can include.

15.3 List a specific example of each of the three broad classes of controls from those given in Table 15.3.

15.4 List the steps we discuss for selecting and implementing controls.

15.5 List three ways that implementing a new or enhanced control can reduce the residual level of risk.

15.6 List the items that should be included in an IT security implementation plan.

15.7 List and briefly define the elements from the implementation of controls phase of IT security management.

15.8 What checks does the organizational security officer need to perform as the plan is being implemented?

15.9 List and briefly define the elements from the implementation follow-up phase of IT security management.

15.10 What is the relation between change and configuration management as a general systems administration process, and an organization's IT security risk management process?

Problems

15.1 Consider the risk to "integrity of customer and financial data files on system" from "corruption of these files due to import of a worm/virus onto system," as discussed in Problem 14.2. From the list shown in Table 15.3, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost effective.

15.2 Consider the risk to "integrity of the accounting records on the server" from "financial fraud by an employee, disguised by altering the accounting records," as discussed in Problem 14.3. From the list shown in Table 15.3, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost effective.

15.3 Consider the risk to "integrity of the organization's Web server" from "hacking and defacement of the Web server," as discussed in Problem 14.4. From the list shown in Table 15.3, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost effective.

15.4 Consider the risk to "confidentiality of techniques for conducting penetration tests on customers, and the results of these tests, which are stored on the server" from " theft/breach of this confidential and sensitive information," as discussed in Problem 14.5. From the list shown in Table 15.3, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost effective.

15.5 Consider the risk to "confidentiality of personnel information in a copy of a database stored unencrypted on the laptop" from "theft of personal information, and its subsequent use in identity theft caused by the theft of the laptop," as discussed in Problem 14.6. From the list shown in Table 15.3, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost effective.

15.6 Consider the risks you determined in the assessment of a small public service agency, as discussed in Problem 14.7. From the list shown in Table 15.3, select what you believe are the most critical risks, and suggest some suitable specific controls that could reduce these risks. Indicate which you believe would be most cost effective.