Topics in This Chapter:

- How Security Supports Organizational Mission, Goals, and Objectives
- Risk Management
- Security Management
- Personnel Security

The *International Information Systems Security Certification Consortium* (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Information Security Governance and Risk Management in this way:

The Information Security Governance and Risk Management domain entails the identification of an organization's information assets and the development, documentation, implementation and updating of policies, standards, procedures and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify the threats, classify assets, and to rate their vulnerabilities so that effective security measures and controls can be implemented.

The candidate is expected to understand the planning, organization, roles and responsibilities of individuals in identifying and securing an organization's information assets; the development and use of policies stating management's views and position on particular topics and the use of guidelines, standards, and procedures to support the policies; security training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary and private information; third-party management and service level agreements related to information security; employment agreements; employee hiring and termination practices; and risk management practices and tools to identify, rate, and reduce the risk to specific resources.

Key areas of knowledge:

- *Understand and align security function to goals, mission, and objectives of the organization*
- *Understand and apply security governance*
- *Understand and apply concepts of confidentiality, integrity, and availability*
- *Develop and implement security policy*
- *Manage the information life cycle (e.g., classification, categorization, and ownership)*
- *Manage third-party governance (e.g., on-site assessment, document exchange and review, process/policy review)*
- *Understand and apply risk management concepts*
- *Manage personnel security*
- *Develop and manage security education, training, and awareness*
- *Manage the security function*

Even though this domain is positioned as number 3 in the Certified Information Systems Security Professional (CISSP) common body of knowledge, it is placed first in this book because all security activities should take place as a result of security and risk management processes.

Organizational Purpose

In order to protect an organization's assets, it is first necessary to understand several basic characteristics of the organization, including its goals, mission, and objectives. All of these are statements that define what the organization desires to achieve and how it will proceed to achieve them. These three terms are described in more detail as follows:

Mission

The mission of an organization is a statement of its ongoing purpose and reason for existence. An organization usually publishes its mission statement, so that its stakeholders, including employees, customers, suppliers, shareholders, and owners, share a common understanding of the organization's stated purpose. Some example mission statements:

> *"Support and provide members and constituents with credentials, resources, and leadership to secure information and deliver value to society."*—(ISC)²
>
> *"Global cryptologic dominance through responsive presence and network advantage."*—United States National Security Agency
>
> *"Organize the world's information and make it universally accessible and useful."*—Google
>
> *"Facebook's mission is to give people the power to share and make the world more open and connected."*—Facebook

As security professionals, we need to be aware of our organization's mission, because it will, in part, influence how we will approach the need to protect the organization's assets.

Objectives

Objectives clearly define the results an organization and its managers want to achieve in a specific time frame. Objectives reflect the broader purposes given by the mission statement and provide specific, observable, and measurable outcomes. Stakeholders periodically review the organization's results by comparing them to the objectives. This process determines the success of the organization and its management. Objectives state strategic priorities. When these are distilled into specific, achievable steps, they become goals.

Sample organization objectives include:

> *"Become the world's leading business human capital management company."*
>
> *"Reduce delayed flight departures to less than 5% of all scheduled flights."*
>
> *"Achieve the lowest personnel turnover in field sales."*

Security personnel need to understand and use the organization's objectives to guide their plans. Security often impedes activities needed to achieve objectives. Achieving the proper balance between security and operations requires evaluating threats through the lens of risk. The optimum solution allows employees to reach goals and achieve the organization's objectives with a minimum amount of risk to confidential data.

Goals

While objectives describe desired outcomes for an organization, goals specify specific accomplishments that will enable the organization to meet its objectives.

Some sample organization goals are:

> *"Obtain ISO 27001 certification by the end of third quarter."*
>
> *"Reduce development costs by twenty percent in the next fiscal year."*
>
> *"Complete the integration of CRM and ERP systems by the end of November."*

Security Support of Mission, Objectives, and Goals

Security professionals support an organization's mission, objectives, and goals by developing processes, practices, and procedures for protecting assets. They assess threats and develop mitigation steps in the context of probability, or risk, that a potential threat can occur. Effective security policy requires including this important consideration in every significant organizational decision. *Forbes* cited a PricewaterhouseCoopers survey showing a significant increase in employment of chief security officers. The report indicated that 41 percent of companies employed a CSO compared to 27 percent one year earlier. Employment of chief information security officers rose from 29 to 44 percent (Greenberg, 2008). Security programs fail without executive support, and the presence of security professionals in the organization's highest management levels reflects the growing importance of this field.

This is discussed in greater detail later in this chapter in the Security Management section.

Risk Management

Risk management is the process of minimizing potential losses. Even though a potential for loss always exists, many can be minimized or avoided. In the event a loss occurs, risk management practices determine how to reduce the costs. Since the potential for loss always exists, the key is to determine the probability or level of risk from a potential threat, scenario, or activity and determine its acceptability. Risk assessment techniques determine the level of risk and determine if the level of risk exceeds an organization's risk tolerance. In that case, the next step requires the development of a strategy to ameliorate specific risks in order to achieve an acceptable level of overall risk to the organization. In the vernacular this means: find the level of risk (associated with a given activity or asset) and improve if needed.

The National Institute of Standards and Technology (NIST) defines four risk management processes—framing, assessing, monitoring, and responding—in Special Publication 800-39. NIST develops security standards for U.S. government agencies, and these publications often assist private-sector organizations with risk management planning.

Risk Management Principles

Risk Assessment

Risk assessments are activities that are carried out to discover, describe, analyze, and evaluate risks. Risk assessments may be qualitative, quantitative, or a combination of these.

Internal audit is related to risk assessment; internal audit is discussed in a separate section in this chapter.

Qualitative Risk Assessment A qualitative risk assessment occurs with a predefined scope of **assets** or activities. Assets can, for example, consist of software applications, information systems, business equipment, business processes, or buildings. Activities may consist of actions or tasks carried out by an individual, group, or department.

A qualitative risk assessment collects descriptive information, including information that cannot be reduced to measurable values. It will typically identify a number of characteristics about an asset or activity, including:

- *Classification*. Assets may be classified according to risk level, business function, or the sensitivity or criticality of data stored or processed by an asset.
- ***Vulnerabilities***. These are weaknesses in design, configuration, documentation, procedure, or implementation.
- ***Threats***. These are potential activities that would, if they occurred, exploit specific vulnerabilities and result in a security incident.
- *Threat probability*. An expression of the likelihood that a specific threat will be carried out, usually expressed in a Low-Medium-High or simple numeric (1–5 or 1–10) scale. In a qualitative risk assessment, this is not a numeric probability but an arbitrary ranking of probability, as a way of distinguishing low probability from high probability.
- *Impact*. An expression of the influence upon the organization if a threat was carried out.
- ***Countermeasures***. These are actual or proposed measures that reduce the risk associated with vulnerabilities or threats.

Here is an example. A security manager is performing a qualitative risk assessment on assets in an IT environment. For each asset, the manager builds a chart that lists each threat, along with the probability of realization. The chart might resemble the list in Table 1-1.

This is an oversimplified example, but sometimes qualitative risk analysis won't be much more complicated than this—although a real risk analysis should list many more threats and countermeasures.

Quantitative Risk Assessment Although qualitative criteria do provide guidance for assessing and evaluating risks, quantitative assessments treat these conditions as discrete mathematical valuations. Often quantitative risks produce stronger arguments for security policies and encourage leaders to support aggressive implementation of security controls. A quantitative risk assessment can be thought of as an extension of a qualitative risk assessment.

Threat	Impact	Probability	Countermeasure	Probability with Countermeasure
Flooding	H	L	Water alarms	L
Theft	H	L	Key card, video surveillance, guards	L
Earthquake	M	M	Lateral rack bracing; attach all assets to racks	L
Logical intrusion	H	M	Network-based intrusion detection system; host-based intrusion detection system	L

Table 1-1 Risk assessment chart

A quantitative risk assessment will include the elements of a qualitative risk assessment but will contain additional items, including:

- *Asset value*. Usually this is a dollar figure that may represent the replacement cost of an asset, but it could also represent income derived through the use of the asset.
- ***Exposure factor (EF)***. The proportion of an asset's value that is likely to be lost through a particular threat, usually expressed as a percentage. Another way to think about exposure factor is to consider the *impact* of a specific threat on an asset.
- ***Single loss expectancy (SLE)***. This is the cost of a single loss through the single event realization of a particular threat. This is a result of the calculation:

$$\text{SLE} = \text{asset value (\$)} \times \text{exposure factor (\%)}$$

- ***Annualized rate of occurrence (ARO)***. This is the probability that a loss will occur in a year's time. This is usually expressed as a percentage, which can be greater than 100% if it is believed that a loss can occur more than once per year.
- *Annual loss expectancy (ALE)*. This is the yearly estimate of loss of an asset, calculated as follows:

$$\text{ALE} = \text{ARO} \times \text{SLE}$$

Let's look at an example: an organization asset, an executive's laptop computer that is worth $2,000. The asset value is $2,000.

Now we will calculate the exposure factor (EF), which is the proportion of the laptop's value that is lost through a particular threat. The threat of theft will, of course, result in the entire laptop's value to be lost. For theft, EF = 100%. For sake of example, let's add another threat, that of damage, if the executive drops the laptop and breaks the screen. For that threat, the EF = 50% (presuming a $1,000 repair bill to replace the LCD screen).

For theft, the single loss expectancy (SLE) is $2,000 × 100% = $2,000. For damage, the SLE is $2,000 × 50% = $1,000.

Now we need to calculate how often either of these scenarios might occur in a single year. For theft, let us presume that there is a 10% probability that this executive's laptop will be stolen. Thus, the ARO = 10%. This particular executive is really clumsy and drops his laptop computer a lot, so the ARO for the threat of accidental damage is 25%.

The annual loss expectancy (ALE) for theft is 10% × $2,000 = $200.

The ALE for accidental damage is 25% × $1,000 = $250.

This all means that the organization may lose $450 ($200 for theft and $250 for damage) each year in support of the executive's laptop computer. Knowing this will help managers make more intelligent spending decisions for any protective measures that they feel will reduce the probability or impact of these and other threats. An example of such a measure is a remote wipe capability for laptop computers and smartphones.

Quantifying Countermeasures **Annual loss expectancy (ALE)** is the cost that the organization is likely to bear through the loss or compromise of the asset. Because ALE is expressed in dollars (or other local currency), the organization can now make decisions

regarding specific investments in countermeasures that are designed to reduce the risk. The risk analysis can be extended to include the impact of countermeasures on the overall risk equation:

- *Costs of countermeasures*. Each countermeasure has a specific cost associated with it. This may be the cost of additional protective equipment, software, or labor costs.
- *Changes in exposure factor*. A specific countermeasure may have an impact on a specific threat. For example, the use of an FM-200-based fire extinguishment system will mean that a fire in a business location will cause less damage than a sprinkler-based extinguishment system, but it is more expensive to reload.
- *Changes in single loss expectancy*. Specific countermeasures may influence the probability that a loss will occur. For instance, the introduction of an advanced malware protection appliance will reduce the frequency of successful malware attacks.

Geographic Considerations Organizations can take quantitative risk analysis a step or two further by calculating SLE, ALE, and ARO values in specific geographic locations. This is useful in organizations with similar assets located in different locations where the probability of loss or the replacement cost of these assets varies enough to be identified.

Specific Risk Assessment Methodologies The risk assessment steps described in this section are purposely simplistic, with the intention of illustrating the concepts of identifying the value of assets and by using formulas to arrive at a quantitative figure that represents the probable loss or compromise of assets in a year's time. For some organizations, this simple approach may be sufficient. On the other hand, there are several formal approaches to risk assessment that may be suitable for larger or more complex efforts. Among these approaches are:

- *OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)*. Developed by Carnegie Mellon University's Software Engineering Institute (SEI), OCTAVE is an approach where analysts identify assets and their criticality, identify vulnerabilities and threats, evaluate risks, and create a protection strategy to reduce risk.
- *FRAP (Facilitated Risk Analysis Process)*. This is a qualitative risk analysis methodology that can be used to prescreen a subject of analysis as a means to determine whether a full-blown quantitative risk analysis is needed.
- *Spanning Tree Analysis*. This can be thought of as a visual method for identifying categories of risks, as well as specific risks, using the metaphor of a tree and its branches. This approach would be similar to a Mind Map for identifying categories and specific threats and/or vulnerabilities.
- NIST 800-30, *Risk Management Guide for Information Technology Systems*. This document describes a formal approach to risk assessment that includes threat and vulnerability identification, control analysis, impact analysis, and a matrix depiction of risk determination and control recommendations.

Risk Treatment

When a qualitative or quantitative risk assessment is performed, an organization's management can begin the process of determining what steps, if any, can be taken to manage the risks identified in the risk assessment. The four general approaches to risk treatment are:

- Risk acceptance
- Risk avoidance
- Risk mitigation
- Risk transfer

It is important to remember that the objective of risk treatment is typically not to eliminate risk—often risk cannot be completely eliminated, but only managed.

Risk Avoidance The associated activity that introduces the risk is discontinued. For instance, an organization performs a risk analysis of an Internet-based shopping cart application, and then decides to abandon the use of the application altogether. This is **risk avoidance.**

Risk Mitigation This involves the use of countermeasures to reduce the risks initially identified in the risk analysis. Examples of **risk reduction** in information systems include firewalls, intrusion detection systems, access reviews, and DMZ networks.

Risk Acceptance In a typical risk assessment, there will be many identified risks, typically ranked as high, medium, and low risk. In an organization with scarce resources, management may choose to forego mitigation of all of the risks ranked low, in other words leaving things as they are and accepting the stated risks. This is known as **risk acceptance.** Occasionally, medium and high risks will also be accepted, although such a decision usually requires more thoughtful consideration as well as formal management approval.

Risk Transfer **Risk transfer** typically involves the use of insurance as a means for mitigating risk. For instance, a risk analysis on the use of laptop computers may identify theft as one risk. While the organization may mitigate the risk through the use of cable locks, it may transfer part of the risk to an insurance company. Note that risk transfer usually involves a cost (insurance premiums) that should be considered in a quantitative risk analysis.

Residual Risk In any particular risk situation, generally only some of the risk can be avoided, reduced, or transferred. There is always some remaining risk, called **residual risk.** Typically this risk must be accepted, unless management can enact another round of analysis and a fresh set of countermeasures to avoid, reduce, or transfer the risk. But even then, there will typically be some "leftover" risk, called *residual risk*.

Security Management Concepts

As security moved from a task to a standalone professional discipline, practitioners developed a de facto framework of foundational concepts. These include:

- Security controls
- CIA Triad
- Defense in depth
- Single points of failure
- Fail open, fail closed, fail soft
- Privacy

The ISO 27001 standard, "Information Technology—Security Techniques—Information Security Management Systems—Requirements," is a respected standard for information security management. Originally developed as British Standard 7799, the standard was adopted by the International Standards Organization (ISO) in 2000. ISO 27001 was later updated in 2005. ISO 27001 is a top-down process approach to security management that requires continuous improvement in an organization's security management system.

Security Controls

Security controls are the measures that are taken to reduce risks through the origination and enforcement of **security policies**. The types of controls used are detective, deterrent, preventive, corrective, recovery, and compensating. These controls are discussed in detail in Chapter 3, "Software Development Security."

The CIA Triad

The core principles of information security are confidentiality, integrity, and availability, often coined as **CIA**. All other concepts and activities in information security are based on these principles. The CIA Triad is depicted in Figure 1-1.

Confidentiality The principle of confidentiality asserts that only properly authorized parties can access information and functions.

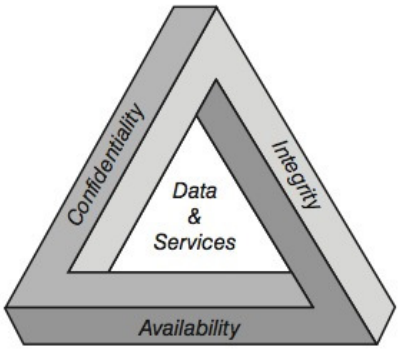

Figure 1-1 The CIA Triad

© 2010 Cengage Learning®

Mobile devices can access information and entertainment for someone at any time or place. However, the freedom of mobility threatens the freedom to keep some aspects of life private. Government agencies and private-sector companies like Google and Facebook collect the data people send across the Internet. These prying eyes place the idea of confidentiality at risk, because individuals cannot control the use of their information or who can look at it.

Individuals expect that their confidential information will not be disclosed to unauthorized parties and that it will be properly protected. However, we have come to expect that some organizations will not handle information properly, resulting in an unauthorized disclosure that, in its worst case, could result in an attempted identity theft or financial fraud carried out against the persons whose information was compromised. The Target stores breach of 2013 is an example of a widespread data compromise.

Integrity The principle of integrity asserts that information and functions can be added, altered, or removed only by authorized persons and means.

The general expectation of information systems is that information will be properly and accurately introduced into a system, and throughout its lifetime the information will remain accurate. While the principle of confidentiality states that only authorized parties will be able to view information, the principle of integrity states that only authorized parties will be able to modify information. Integrity is achieved through role-based access control, which is the generic name for a mechanism that defines and limits the actions individuals may perform. In the context of information stored in a database, which consists of tables, rows, and fields, the concept of integrity will govern which individuals are able to modify which tables, rows, and fields in the database.

In data security, the need for integrity encompasses software, systems, networks, and the people who design, build, and operate them. Software must be correctly developed, configured, and maintained and must operate properly, particularly when a program is accessing and modifying data. Systems must be properly configured so that the data that resides on them is managed and updated correctly. The people who design, build, and operate software and systems must be properly trained on the technologies that they are using, and they must also adhere to a code of professional ethics that guides their behavior and decision-making.

Availability The principle of availability asserts that systems, functions, and data must be available when an authorized user needs to access them. Different levels of availability exist based upon predefined parameters regarding levels and types of service.

Availability is multifaceted and involves many separate safeguards and mechanisms to ensure that systems and data are available when needed. These safeguards range from preventing damage through the use of firewalls, anti-virus software, and surge protectors to redundant architectures used for business continuity and disaster recovery. Availability requires planning and includes change and configuration management. Availability covers nearly all of the aspects of data security that directly or indirectly protect a system from harm.

Defense in Depth

The term **defense in depth** implies a *layered defense* consisting of two or more protective methods that protect some asset. According to the National Security Agency, defense in

depth defines a process for balancing protection capability, cost, performance, and operations considerations (National Security Agency, 2013). Some of the characteristics of defense in depth are:

- *Heterogeneity*. A good defense in depth mechanism may contain different types of protective mechanisms. For example, two layers of firewalls of different brands.
- *Holistic or comprehensive protection*. Each layer of the defense fully protects an asset against the type of threat that the defense is designed to block. For example, anti-virus on an e-mail server and also on end-user workstations.

The classic example of a good defense in depth is the medieval castle's defenses that include a drawbridge, a moat, a moat monster, archers, soldiers to pour boiling oil, and so on. These defenses are all different from one another but are all designed to protect the castle (and its assets) from attack from outsiders. Each defense operates on its own and does not require others for it to properly function.

The objective of defense in depth is to reduce the probability that a threat can act upon an asset. This occurs in three ways:

- *Single vulnerability*. If one of the components of a defense in depth had an exploitable vulnerability, chances are that another layer in the defense will not have the same vulnerability.
- *Single malfunction*. If one of the components of a defense in depth malfunctions, chances are that another layer in the defense will not malfunction.
- *Fail open*. If one of the components in a defense in depth fails open, the other component(s) will continue to operate and protect the asset.

Single Points of Failure

A **single point of failure** is the characteristic of an individual component in a system if the failure of the component will result in the failure of the entire system.

Single points of failure are generally discussed only in a system that is designed for resilience and that contains redundant components. A single point of failure in such a system would be any portion of the system where redundancy does not exist.

For example, the firewall in Figure 1-2 would be a single point of failure. If the firewall fails, the system will be unreachable. The firewall is a single point whose failure will cause the failure of the entire system's objectives.

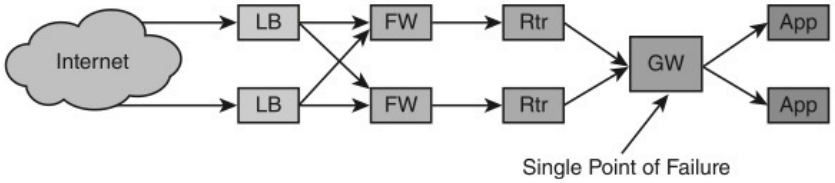

Figure 1-2 Single point of failure in an otherwise resilient environment

© 2010 Cengage Learning®

Fail Open, Fail Closed, Fail Soft

The concepts of *fail open*, *fail closed*, and *fail soft* are related to what happens to the protection in the event of a failure of a security control.

When a security control fails, generally one of two things happens: either the control blocks all access, or it permits all access. If the control fails and it blocks all access, it is said to **fail closed**. Another term for fail closed is **fail safe.**

If the control fails and permits all access, it **fails open**.

A system can take action during an adverse situation such as a hardware failure. **Fail soft** is the process of shutting down nonessential components on a system, thereby freeing up resources so that critical components can continue operating.

Generally speaking it is more desirable for a control to fail closed than to fail open. This, however, is dependent upon the objective and design of the entire system.

An example of undesirable fail open is a doorway controlled by a key card access system that can be bypassed if the key card system fails. A desirable fail open would be the automatic opening of security doors to facilitate personnel exiting in case of fire.

Most security controls fail closed. For example, if a key card system fails, personnel cannot enter or move about the premises. If an application server is unable to access an LDAP authentication server, then no users can log on to the application.

Privacy

The Merriam-Webster dictionary defines **privacy** as "freedom from unauthorized intrusion." Wiktionary defines privacy as "the state of not being seen by others." The practice of privacy in business refers to the protection of individuals' private information so that it is used only for intended and agreed-upon purposes, as well as being protected from unauthorized disclosure.

Personally Identifiable Information Personally identifiable information (PII) refers to the items that comprise a person's identity, usually including:

- Full name
- National identification number (in the United States, social security number)
- Telephone number
- Driver's license number
- Passport number
- Residential address
- Bank account numbers
- Credit card numbers

In many locales, organizations are required to protect many of, or combinations of, these items, and sometimes others, from unauthorized disclosure. Organizations are also usually required to disclose all uses of private information, as well as the parties to whom they send this information. Most often these requirements are in the form of laws and regulations

intended to curb the proliferation of this information to others. The objective of these laws and regulations is the prevention of identity theft, fraud, and harassment by those who might obtain a person's PII.

Security Management

Security management is primarily concerned with strategic-level activities that influence the operation of systems and the behavior of employees. Security management involves several key activities, including:

- Executive oversight
- Governance
- Policy, guidelines, standards, and procedures
- Roles and responsibilities
- Service level agreements
- Secure outsourcing
- Data classification and protection
- Certification and accreditation
- Internal audit

Security Executive Oversight

The support and oversight by executives of security-related activities is vital to the viability of a security program in an organization. Several activities are related to this oversight, including:

- *Support of policies*. Executive support is needed to ensure that security policies and other policies are taken seriously by all members of the organization. Support should come in the form of communication (memos stating that adherence to policy is a required condition of employment) and leadership by example.
- *Allocation of resources*. Executives control the allocation of resources in an organization, primarily through budgeting and staffing levels. In order for a security program to be effective, executives must allocate sufficient resources to security.
- *Support of risk management*. One of the primary activities in a security management function is the performance of risk assessments, which result in the treatment of identified risks. Executives need to formally accept the disposition of risks as documented in risk assessments whether risks are accepted, transferred, mitigated, or avoided.

Security Governance

The IT Governance Institute in its *Board Briefing on IT Governance, 2nd Edition*, defines security **governance** this way:

> *"Security governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic*

> *direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly."*

In other words, strategy, objectives, and risks are developed and executed in a top-down manner. In a governance model, executive management is in control of the activities intended to protect organization assets from known threats. Usually this translates into a series of activities that include:

- *Steering committee oversight*. A group of executives are regularly briefed on activities related to security and risk management. Discussions about incidents and events take place, changes to policies are made, and decisions and opinions are solicited.
- *Resource allocation and prioritization*. Executives allocate resources to security-related activities in order that required activities may be carried out.
- *Status reporting*. Information about events, trends, issues, and other security-related matters are collected and sent to upper management through status reports that provide feedback on decisions, strategic direction, and overall effectiveness of the security program.
- *Decisions*. Decisions made at the steering committee level (and at lower levels) are sent downwards to appropriate levels to be carried out by managers and staff members.

Security Policies, Requirements, Guidelines, Standards, and Procedures

Organizations establish documented processes for managing their security profiles. Taking a formal approach increases costs, generally substantiated by regulatory compliance or reduced civil liability. Security programs consist of policies, requirements, guidelines, standards, and procedures that address human and systems behavior. They define acceptable standards and usage and detail consequences for violations. Formal processes provide the organization with a consistent set of standards and methods for handling individuals and incidents. They also detail the frequency of audits and periodic policy reviews.

Policies, requirements, guidelines, standards, and procedures are a hierarchy, where policies are very general statements of *what* should be done. Requirements, guidelines, standards, and procedures are much more specific and describe *how* policies should be carried out. Because of this, a well-written set of policies will not need to be changed very often, while requirements, guidelines, standards, and procedures may need to be changed more frequently.

Policies Security **policies** describe constraints of behavior for an organization's personnel as well as the acceptable use of its information systems, data, and other mechanisms. Put another way, security policy specifies the activities that are required, limited, or forbidden in an organization.

An example policy is, *Information systems should be configured to require compliant security practices in the selection and use of passwords.*

Policy Standards The international standard, ISO 27002:2013, *Information technology—Security techniques—Code of practice for information security management*, is a well-known

framework on which an organization can build its security policy. The sections in the standard are:

- Information security policies
- Organization of information security
- Human resources security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- Systems acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance; with legal requirements, such as policies, and with external requirements, such as laws

The SANS organization has a well-known security policy model in the *SANS Security Policy Project* found at http://www.sans.org/security-resources/policies/. Here the reader can find articles on policies, standards, guidelines, example policies, and white papers on the development of security policy.

Policy Effectiveness An organization that enacts policies should take steps to ensure that its policies are effective. Policy effectiveness requires a top-down approach. To be effective, a security policy must be:

- Approved by senior management
- Communicated to employees
- Periodically reviewed
- Assessed for effectiveness

Security policy must reflect and support the mission, objectives, and goals of an organization. If the organization is risk-averse, then its security policy should support risk aversion. If the organization has a greater appetite for risk, then its security policy should reflect this also.

Requirements The term **requirements** usually refers to characteristics of an information system or business process. Typically, a set of requirements will be created when a new information system is being developed or purchased. The requirements will help the organization make suitable selection, design, or configuration decisions.

Requirements should reflect security policy; if security policy says, "a system shall be configured to prevent unauthorized access," then a corresponding requirement would specify how this is accomplished. In this instance the requirement might state that users must lock out

their systems when they leave the work area and also specify that system configurations automatically lock out after two minutes of inactivity. Notice how the requirement fulfills the policy with specific actions addressing human behavior and systems configuration, which compensates for human failure. The goal of security requirements is to constrain a system or process so that, when implemented, it complies with the organization's security policy.

Another example of a requirement is, *Information systems must enforce password quality standards and must be able to reference a central authentication service, either LDAP or Active Directory.*

Guidelines Whereas security policy defines *what* should be done (or not done), **guidelines** provide information on *how* policy can be implemented. Generally, guidelines are suggestions or ideas on how specific policies may be implemented. Which approach (including a blended approach) is adopted is up to the organization.

For example, if a security policy states that *personnel access to business facilities shall be controlled*, guidelines can suggest that key card systems with PIN pads be used at building entrances and within sensitive areas inside buildings.

An example guideline is, *Users should choose a password that is easy for the user to remember, but hard for others to guess. The types of passwords that should be avoided include: employee, spouse, or pet names, significant anniversaries, common words such as "password," words related to work functions, and other easily guessed words.*

Standards **Standards** are statements that specify *what* shall be used to support security policies and guidelines. Typically, standards will comprise the following:

- *Product standards*. These are specific names of products that shall be used to support a policy.
- *Process standards*. These may cite process templates, names, or methodologies.
- *Technology standards*. This includes the use of technology standards such as TCP/IP or OSPF, computer languages, and so on.
- *Reference configurations*. These include server build specs, router configurations, software configurations, hardening specifications, and so on.
- *Reference architectures*. These include schematics for building networks, specifications for integrating applications, and so on.

It is expected that standards will change far more frequently than policies and guidelines.

An example standard is: *Minimum password length is 8 characters. Passwords must consist of lower case, upper case, and numeric characters. Passwords shall expire after no more than 90 days. Accounts must automatically lock if a user has entered an incorrect password more than three times in ten minutes; accounts must be unlocked by an access administrator, or may be automatically unlocked one hour after the last logon attempt. Users may not use any of the previous 10 passwords used.*

Procedures **Procedures** are the instructions that specify *how* tasks are to be performed. True to the hierarchical form, procedures must support policies, guidelines, and standards.

The purpose of a procedure is to ensure the consistent and methodical completion of repetitive tasks. Consistency builds quality and reduces incidents, which allows the organization to operate more efficiently and at greater levels of service.

Security Roles and Responsibilities

Management should define security roles and responsibilities in the organization. This includes not only the roles and responsibilities of dedicated security personnel, but of all employees in the organization. Roles and responsibilities should be formally defined in two places:

- ***Security policy***. General and specific expectations of security staff and other employees should be defined in the organization's security policy.
- *Job descriptions*. Individual job descriptions of security staff and other employees should define specific security-related roles and responsibilities.

The roles and responsibilities that need to be defined include:

- *Ownership of assets*. Individual assets and groups of assets need to have designated owners who are responsible for their operation and protection.
- *Access to assets*. The owners of assets should be designated as the persons who decide who may access or use those assets. A higher level of management may be responsible for approving nonstandard access to assets.
- *Use of assets*. All employees should be explicitly designated as responsible for their individual use of assets.
- *Managers*. Managers should be designated as being responsible for the behavior of employees under their control.

Service Level Agreements

A **service level agreement (SLA)** is a formally defined level of service provided by an organization. Within the context of security management, SLAs may be defined for many activities, including:

- *Security incident response*. A security team may be required to mobilize within a stated period of time when a security incident has been called.
- *Security alert delivery*. Security alerts, which may be bulletins of threats or vulnerabilities, may need to be delivered to recipients within a stated period of time.
- *Security investigation*. A security investigator may be required to respond to a call for assistance within a stated period of time.
- *Policy and procedure review*. A security team may be required to periodically review policies, procedures, and other documents at regular intervals.

SLAs can be defined for other tactical activities performed by security management and staff.

Secure Outsourcing

Outsourcing is the subcontracting of a business process to a third-party company. Organizations outsource many different functions for a variety of reasons, including:

- Redirecting energy to the organization's core competencies
- Controlling the efficient use of capital and other resources

There are some risks associated with the outsourcing of business processes to third parties, including:

- *Control of confidential information*. An organization will need to equip the third-party provider with the information required to perform its functions properly. Because this information is now out of its direct control, protection of that information is now entirely dependent upon the outsourcer's actions.
- *Loss of control*. Organizations that outsource functions to third parties give up a measure of control to that organization.
- *Accountability*. While the organization has outsourced functions to a third party and is at the complete mercy of the third party's integrity, the organization is still completely accountable for the actions performed by the vendor.

Organizations with a large number of outsourcing relationships may need to develop an outsourcing classification scheme that categorizes each supplier according to one or more criteria, including:

- Sensitivity of the data it processes for the organization
- Volume of data it processes for the organization
- Criticality of the business process(es) supported in the organization

These classifications will help the organization determine what measures are necessary to confirm that each supplier is performing its activities correctly and that it is adequately protecting the organization's information.

Additional terms related to the practice of outsourcing include:

- ***Insourcing***. The use of internal staff to perform a business function.
- ***Offshoring***. The use of internal or external staff in another country.
- ***Onshoring***. The use of internal or external staff within a country.

Note that outsourcing and insourcing are related to whether an organization uses its own staff to perform business functions, while the terms offshoring and onshoring are related to the location of insourced or outsourced personnel.

Data Classification and Protection

Organizations store, transmit, and manage a wide variety of types of information, ranging from personnel and payroll records to computer source code to content on public-facing web sites. Information security professionals who are responsible for protecting this information need to decide what measures are required to protect the data. Data of widely varying levels of sensitivity exists in many forms; while it is possible to develop criteria for protecting every set of data in the organization, this approach scales poorly.

Data classification is the undertaking of developing levels of sensitivity for information, and assigning those levels for the purpose of establishing appropriate modes of protection for those data sets. This orderly system of assigning classification levels is preferable to a chaotic environment where information is protected in an ad hoc style.

A formal data classification program consists of several parts, which are:

- Sensitivity levels

- Marking procedures
- Access procedures
- Handling procedures
- Destruction procedures

Sensitivity Levels In a data classification program, a set of **sensitivity levels** is established, which reflects the nature of data that is used in the organization. Such a set of sensitivity levels could be, for example:

- Top Secret
- Secret
- Confidential
- Restricted
- Official
- Unclassified
- Public

Most organizations don't have more than four or five levels, since each level generally will have its own sets of marking and handling procedures. The more levels there are, the more complicated the classification program will be. Pragmatically, establishing too many levels will introduce unnecessary complications, increasing the likelihood of errors, while providing only marginally more security than a simpler program. A data classification program that is too complex may be ignored altogether if personnel are unsure of how to carry it out or the requirement is too onerous.

Because information classification and handling is largely a human-driven and -operated process, it is preferable to use a simpler scheme of classification levels that will encourage compliance and reduce ambiguity and errors.

Information Labeling Labeling, or **marking**, is the process of affixing a word, symbol, or phrase on a set of data. The purpose of labeling is to make other readers aware of the level of classification on a set of data. When others are aware of the classification level of a particular set of data, they are more apt to be aware of the classification level and handle the data properly.

Using the example of the four levels of classification above, here are some sample labels that can be affixed to human-readable documents, shown in Table 1-2.

Marking is not as simple as it may first appear. While it can be relatively simple to mark a document or report with a header or footer containing a classification word or phrase, or affix a classification label on a backup tape, effectively labeling stored or transmitted data is not so clear-cut. Other situations include:

- *On-screen labeling*. Software programs that display classified information can include on-screen labeling.

Level	Label
Top Secret	"COMPANY Top Secret" in at least 48 pt type on cover page. "COMPANY Top Secret: for registered personnel only" in at least 24 pt type on every page.
Secret	"COMPANY Secret: for authorized personnel only with a business need-to-know" in at least 20 pt type on every page.
Confidential	"COMPANY Confidential: for employees and customers only" in at least 14 pt type on every page.
Public	"COMPANY Approved for Public Use" on every page.

Table 1-2 Sample classification labels

- *Data transmission*. Devices that transmit classified information can have labels affixed to them; further, administrative interfaces (used by network or systems engineers) can have a label displayed at login time. Cabling used to transmit classified information can be labeled or color-coded.

Handling Once information is introduced into an organization, it needs to be appropriately categorized and properly handled in every type of situation. Handling guidelines need to be developed for each level of classification, for each possible type of activity, including these listed here and possibly several more:

- *Computer storage*. Classification guidelines can include which systems (or classes of systems) are permitted to store the data and under what specific conditions.
- *Computer access control*. Classification guidelines may include business rules about which personnel (individuals, groups, departments, roles, security clearance level, etc.) may access classified information.
- *Backup tape and other portable media*. Classification guidelines will determine when and how data at different classification levels may be written to various types of portable media. For instance, data at the highest levels of secrecy might be forbidden from most or all portable media, and at other levels, encryption may be required.
- *Network transmission*. Classification guidelines should specify if and how data at various classification levels may be transmitted over networks. Of course there are different types of networks (internal, external, and perhaps physically separate high-secrecy networks), so this guideline alone will probably be multidimensional.
- *E-mail transmission*. Classification guidelines may determine which classification levels permit e-mail to be used to transmit classified information to another person. Like network transmission, e-mail transmission will probably contain conditions such as encryption, internal versus external recipients, and so on.
- *Facsimile*. Classification guidelines should address whether information at different classification levels can be faxed and, if so, what conditions should be imposed, such as confirming that the sender's and recipient's fax machines will be attended throughout the transmission.
- *Printing*. Classification guidelines should address the conditions under which information at various classification levels may be printed.

- *Mailing/shipping/courier*. Classification guidelines need to address whether and how classified information may be mailed or shipped. Possible conditions include lockbox, registered, insured, and double-sealed packages.
- *Carrying*. Classification guidelines need to include guidance on the safeguards that individuals need to take when carrying classified information.
- *Hard copy storage*. Classification guidelines should address how hard copies of classified information must be stored. Some levels may require double-locking (stored in a locked desk or cabinet in a locked office, for instance).

Destruction Classification guidelines need to include information on the proper disposal of classified information. **Destruction** procedures—steps to ensure that information is discarded in a way that renders it non-retrievable—need to include every type of media and likely context.

For example, media destruction procedures should include proper disposal of hard copy documents. In the workplace there are sure to be shredders or secure document disposal bins, but what about staff members who work primarily in home offices? And how does someone on extended travel safely dispose of a classified document?

Certification and Accreditation

Certification and accreditation are the activities associated with the evaluation of a system against a set of standards or policies. These activities are carried out as part of a formal approval process for initiating or continuing the use of a system.

- **Certification** is the process of evaluating a system against a set of formal standards, policies, or specifications.
- **Accreditation** is the formal approval for the use of a certified system, for a defined period of time (and possibly other conditions).

Internal Audit

In the context of information security, **internal audit** is the activity of self-evaluation of security controls and policies to measure their effectiveness.

In order to be effective, the internal audit function must be objective and independent. This means that the staff members performing internal audit activities should not be a part of the department or division that they are examining. Instead, internal audit should report to a dissociated part of the organization such as Legal.

Internal audit should follow a formal methodology that will further the objectivity and quality of the examination of security controls. Two of the most widely recognized methodologies are:

- Standards and practices of internal auditing from The Institute of Internal Auditors, available at www.theiia.org
- *IT Audit and Assurance Standards, Tools, and Techniques* from the Information Systems Audit and Control Association (ISACA), available at www.isaca.org/standards

Security Strategies

Management is responsible for developing the ongoing strategy for security management. The development and changes to the security strategy will be based upon several factors, including the organization's mission, objectives, and goals; the organization's risk tolerance; applicable security and privacy regulations; security requirements from customers, partners, and suppliers; and the results of past events, including:

- *Incidents*. If any security incidents have occurred, the facts uncovered in the handling of the incident, as well as its root cause, may prompt management to make changes.
- *Performance of SLAs*. If the performance of SLAs is below expectations, management may make changes to improve this.
- *Certification and accreditation*. The outcomes of recent certifications and accreditations may provide cause for strategic changes.
- *Internal audit*. The results of internal audits may prompt management to make changes to audited processes or to the audit process itself.

Strategic changes should be made in consultation with executive management and through the governance function described earlier in this section.

Personnel Security

Organizations are becoming more dependent upon information systems in support of key business processes, and more personnel have access to vast stores of organizational data. The risk of security incidents caused by employees' innocent mistakes as well as deliberate malicious acts cannot be eliminated: personnel require access to information to carry out their duties. Organizations need to protect themselves through effective hiring and personnel management practices that include:

- Prescreening employee backgrounds including checks for arrests, convictions, bankruptcy, and verification of employment and educational credentials
- Requiring workers to sign various agreements aimed at protecting the organization's assets
- Training and testing workers so that they are aware of the organization's security policies and practices
- Enacting common practices to reduce behavioral risk
- Performing effective employment terminations

These topics are addressed in this section.

Hiring Practices and Procedures

The near-universal practice among organizations is the use of written agreements that employers and employees sign at various stages of the employment relationship.

Non-Disclosure Agreement As soon as an employer and an employment candidate are discussing the candidate's potential employment in the organization, the employer may require the candidate to sign a **non-disclosure agreement (NDA)**. This agreement will require that the candidate not discuss any nonpublic details about the organization with any other party.

The advantage of the preemployment NDA is that the employer will have some written assurance that the candidate will not share any information shared during interviews. While an employment agreement will certainly have a non-disclosure clause in it, a separate preemployment NDA provides some protection from disclosure by those individuals whom the organization does not hire but may share sensitive information with during the interview process.

Background Verification As the preemployment relationship advances, an employer that is considering making an offer of employment to a candidate will, in most jurisdictions, be required to obtain a signed consent to obtain background information from the candidate. In this simple form, the candidate is providing basic identifying information (e.g., full name, aliases, date of birth, country of citizenship, social/insurance number), together with a written consent for the employer to obtain background information.

The consent form may also contain a clause that states that the employer may refuse employment, terminate employment, and even turn the candidate over to law enforcement authorities if the candidate provides false or misleading information or is found to have an undesirable background.

The employer may also use information obtained from the employment application form to confirm certain aspects of a candidate's background.

There is increased reliance on the use of electronically stored and delivered information. Thus, there is a higher potential consequence of hiring an employee with a criminal background. An organization that is considering hiring a candidate should complete a **background verification** to validate the truthfulness of the candidate's claims and to investigate the candidate's potential criminal background. The following checks may be included in a background verification:

- Confirmation of citizenship, identity, and the candidate's legal right to employment
- Confirmation of employment history
- Confirmation of education background
- Confirmation of professional certifications and licenses
- Investigation of potential criminal history
- Investigation of credit history, important for positions involving financial management responsibility
- Investigation of potential ties with terrorist or criminal organizations
- Check of professional references

Some organizations also attempt to gather information about a prospective employee's character. Organizations that do this may perform online searches to see what information about the candidate is freely available online. Employers may also search social networking sites such as Facebook, LinkedIn, and Twitter.

Offer Letter An organization intent upon hiring a candidate will next issue an offer of employment, or **offer letter**, which usually contains:

- Position title and description
- Start date
- Compensation
- Name of manager

The offer letter should tie together the other elements of the hiring process, including non-disclosure, background check, non-compete, and the requirement that the candidate always abide by security policy and other policies.

Non-Compete Agreement In some locales, an organization can also restrict an employee's ability to change employers to work for a competitor. Organizations intent on enforcing non-compete are concerned with the protection of their intellectual property and other insider information. A **non-compete agreement** is a legal agreement that specifies terms and conditions related to the possibility of an employee accepting employment with a competing organization in the future.

Intellectual Property Agreement An **intellectual property agreement** guarantees that the organization owns all intellectual property (IP) that may be created by an employee. Often this includes IP that an employee may create while working on his or her own time using his or her own resources.

Employment Agreement Sometimes an organization and a new employee will sign an **employment agreement** that defines terms and conditions of the employment relationship. Where labor unions are sometimes used to manage employer-employee relationships, employment agreements often represent an entire segment of the organization's workforce.

Employee Handbook Many organizations have an **employee handbook**, a formal document that describes the terms and conditions of employment, including but not limited to:

- Working hours and locations
- Expected behavior
- Compensation and benefits
- Paid and unpaid leave
- Policies, including security policy
- Acceptable use of organization assets, including workstations and other information systems

In many situations, employees are required to sign the employee handbook, which provides a written attestation that the employee understands all of the terms and conditions of employment and of the organization's principal policies.

Formal Job Descriptions Many organizations have developed formal **job descriptions**, which are formal documents that typically include:

- Job title

- Pay range
- Description of duties
- Description of responsibilities
- Required experience

Often, organizations include adherence to policies in the list of responsibilities. This further strengthens the organization's message that all policies, including security policies, are taken seriously.

Termination

Various circumstances lead to a separation of employment, which are either employee-initiated or employer-initiated. Regardless of the cause, organizations need to perform certain critical tasks upon **termination** of an employee, including:

- Terminate access to all information systems and networks
- Change administrative passwords that may be known to the employee
- Recover all organization-owned assets
- Have incoming e-mail for the terminated employee routed to a designated person or group

Some termination situations call for an urgent revocation of access by the terminated employee, to prevent the former employee from accessing information systems for the purpose of causing harm to the organization. At times the organization will need to take additional steps, including:

- A review of all recent activities related to the terminated employee
- Code reviews of software source code that the terminated employee had access to
- Change control and configuration management reviews of systems under the control of the terminated employee

These reviews may be needed, on the chance that the employee sensed the termination was imminent and had reason to damage information systems.

Work Practices

Several practices, when put into place, will reduce behavioral-based risk in an organization.

These practices are:

- Separation of duties
- Job rotation
- Mandatory vacations

Separation of Duties The principle of **separation of duties** (sometimes known as *segregation of duties*) states that important tasks should require more than one person to complete. A group of two or more employees are less likely to carry out an unauthorized task. Examples of tasks that should employ separation of duties include:

- Payment requests
- Requests for privileged access

In these examples, no single individual should be able to perform these duties. Instead, strictly controlled processes should be established that require at least two individuals (and not just *any* two, but two designated persons or roles not in a hierarchical reporting relationship with each other) to perform these functions.

Job Rotation Personnel in sensitive roles may, after extended intervals, be tempted to collusion for personal gain and other unauthorized activities. When employers occasionally rotate personnel through various roles, especially when unannounced, employees are less likely to perform these "extra" activities. This practice is known as **job rotation.** Enacting this can be difficult in smaller organizations that have only single individuals in various roles.

Mandatory Vacations While it is laudable that some employees are so loyal to their employers that they wish to never leave their posts, mandatory vacations provide something akin to short-term job rotation that sometimes enables an organization to spot irregularities that may be a sign of unauthorized activities. When mandatory vacations are institutionalized, employees are less likely to carry out prohibited activities that could be detected during their absence.

Security Education, Training, and Awareness

In order to adequately protect their assets, organizations need their employees to exercise due diligence and be keen to irregularities that could be signs of trouble. But because "security common sense" is not yet common (and because organizations' security policies vary from one another), organizations need to take time to teach their employees the "dos and don'ts" of information security. This formal education is known as **security awareness training** and needs to be strategic, formal, and presented in a variety of ways, including:

- *Security content in new-hire paperwork*. This includes the employee handbook and documents that a new employee is required to sign upon hire. This is covered earlier in this chapter in the Hiring Practices and Procedures section.
- *Security content in day-one orientation*. New employees need to be made aware of key security policies on their first day of employment.
- *Security training*. Soon after starting employment, new employees should be enrolled in more comprehensive security awareness training, which may take the form of classroom or web-based training.
- *Specialized training*. Employees in some job categories may be required to attend additional specialized training, including:
  - Secure programming for software developers
  - Fraud prevention for finance department employees
  - Network and system protection for network and system engineers
- *Other messaging*. In addition to training, messages of other forms need to be periodically made available to employees, including:
  - E-mail
  - Posters and flyers
  - Promotions

  - Voice mails
  - Incentive programs
- *Testing*. In addition to providing educational material on security and asset protection, many employers also test employees to assess their knowledge. Employees may even be required to attain a minimum test score or be required to repeat security training.

Chapter Summary

- An organization's security program should support the organization's mission, objectives, and goals.
- *Risk management* is the process of determining the acceptable level of risk and the use of risk assessment and mitigation to reduce risk to an acceptable level.
- The core principles of information security are *confidentiality*, *integrity*, and *availability*.
- *Defense in depth* is a technique of using a layered defense to protect an asset.
- A *single point of failure* is the characteristic of a component in a system if the failure of the component will result in the failure of the system.
- *Fail open* is the characteristic of a control to permit all accesses when the control fails.
- *Fail closed* is the characteristic of a control to block all access when the control fails.
- *Privacy* is related to the protection of private information associated with private citizens.
- Executive oversight is needed for the support of policies, allocation of resources, and support of risk.
- *Security governance* is the set of responsibilities and practices related to the development of strategic direction and risk management.
- *Security policies* specify the required characteristics of information systems and the required conduct of employees.
- *Security requirements* specify required characteristics of information systems and processes and are usually used during systems development and acquisitions.
- *Guidelines* are statements that specify how security requirements may be carried out.
- *Standards* specify the types of systems, tools, technologies, configurations, and architectures used in an organization.
- *Procedures* are the step-by-step instructions used to perform tasks.
- Security-related roles and responsibilities are defined in security policies and job descriptions.
- Security roles and responsibilities define the ownership, access, and use of assets, and the general responsibilities of managers and employees.
- *Service level agreements (SLAs)* are formal statements that specify levels of service provided by a service organization.
- An organization that *outsources* information systems or business processes needs to ensure that its intellectual property, service levels, and operational integrity are adequately protected.

- A *data classification* and protection policy defines levels of sensitivity for business information, as well as handling procedures for each level of sensitivity.
- *Certification* is the process of evaluating a system against a set of evaluation criteria.
- *Accreditation* is the act of permitting the use of a certified system.
- *Internal audit* is the activity of evaluating security controls and policies to measure their effectiveness.
- Management is responsible for the development of security strategies, in order to maintain and improve security-related activities in the organization.
- An organization's hiring process should include the use of non-disclosure, employment, non-compete, intellectual property, and acceptable use agreements, as well as background checks.
- An *employee handbook* should highlight all terms and conditions of employment.
- Job descriptions should explain all responsibilities and requirements for each position in the organization.
- Upon termination of employment, the organization should retrieve all assets issued to the terminated employee and immediately rescind the employee's access to all information systems.
- Sound work practices include separation of duties, job rotation, and mandatory vacations.
- A security education, training, and awareness program should keep employees regularly informed of their expectations.

Key Terms

Accreditation The process of formally approving the use of a system.

Annual loss expectancy (ALE) The yearly estimate of loss of an asset, calculated as ALE = ARO × SLE.

Annualized rate of occurrence (ARO) The probability that a loss will occur in a year's time.

Asset An object of value to the organization. An asset may be a physical object such as a computer, or it can be information.

Availability The concept that asserts that information systems can be accessed and used when needed.

Background verification The process of verifying an employment candidate's employment, education, criminal, and credit history.

Certification The process of evaluating a system against a specific criterion or specification.

CIA Confidentiality, integrity, and availability.

Classification See *data classification*.

Confidentiality The concept of information and functions being protected from unauthorized access and disclosure.

Countermeasure A control or means to reduce the impact of a threat or the probability of its occurrence.

Data classification The process of assigning sensitivity levels to documents and data files in order to assure their safekeeping and proper handling.

Defense in depth A strategy for protecting assets that relies upon several layers of protection. If one layer fails, other layers will still provide some protection.

Destruction The process of discarding information in a way that renders it non-retrievable.

Employee handbook A formal document that defines terms and conditions of employment.

Employment agreement A legal agreement that specifies terms and conditions of employment for an individual employee.

Exposure factor (EF) The proportion of an asset's value that is likely to be lost through the realization of a particular threat.

Fail closed The characteristic of a security control—upon failure, it will deny all access.

Fail open The characteristic of a security control—upon failure, it will permit all access.

Fail safe See *fail closed*.

Fail soft The process of shutting down nonessential components on a system, thereby freeing up resources so that critical components can continue operating.

Governance The entire scope of activities related to the management of policies, procedures, and standards.

Guideline Information that describes how a policy may be implemented.

Insourcing The practice of using internal staff to perform a business function.

Integrity The concept of asserting that information may be changed only by authorized persons and means.

Intellectual property agreement A legal agreement between an employee and an organization that defines ownership of intellectual property (IP) that the employee may develop during employment.

Internal audit The activity of self-evaluation of controls and policies to measure their effectiveness.

Job description A formal document that defines a particular job title, responsibilities, duties, and required experience.

Job rotation The practice of rotating personnel through a variety of roles in order to reduce the risk of unauthorized activities.

Labeling The process of affixing a sensitivity identifier to a document or data file.

Marking See *labeling*.

Non-compete agreement A legal agreement that stipulates terms and conditions regarding whether the employee may accept employment with a competing organization in the future.

Non-disclosure agreement (NDA) A legal agreement that requires one or both parties to maintain confidentiality.

Offer letter A formal letter from an organization to an employment candidate that offers employment under a basic set of terms.

Offshoring The use of internal or external staff in another country.

Onshoring The use of internal or external staff within a country.

Outsourcing A business arrangement where an organization contracts out a business process, which was previously performed internally, to another organization.

Personally identifiable information (PII) Items associated with an individual such as name, passport number, driver's license number, and social security number.

Policy An official statement that establishes plans, boundaries, and constraints on the behavior of information systems and employees.

Privacy The protection of sensitive information associated with individuals.

Procedure Step-by-step instructions for performing a task.

Requirements Statements of necessary characteristics of an information system.

Residual risk The risk that remains after countermeasures are applied.

Risk acceptance A form of risk treatment where an identified risk is accepted as is.

Risk assessment The process of examining a system or process to identify potential risks.

Risk avoidance A form of risk treatment where the activity associated with an identified risk is discontinued, thereby avoiding the risk.

Risk management The strategic activities related to the identification of risks through risk assessment and the subsequent treatment of identified risks.

Risk mitigation See *risk reduction*.

Risk reduction A form of risk treatment where an identified risk is reduced through countermeasures.

Risk transfer A form of risk treatment where an identified risk is transferred to another party, typically through an insurance policy.

Security awareness training A formal education program that teaches security principles and expected behavior to employees.

Security management Activities related to the development and implementation of security policies and controls.

Security policy A branch of organizational policy that defines security-related controls and behaviors.

Sensitivity level A category of information sensitivity in an information classification scheme.

Separation of duties The work practice where important tasks are structured to be carried out by two or more persons.

Service level agreement (SLA) Formal statement that specifies level of service provided by a service organization.

Single loss expectancy (SLE) The cost of a single loss through the realization of a particular threat. This is a result of the calculation SLE = asset value × exposure factor (EF).

Single point of failure A component in a system that lacks a redundant or backup counterpart; the failure of the component will cause the failure of the entire system.

Standard A statement that specifies the brand, model, protocol, technology, or configuration of a system.

Termination The cessation of employment for an employee.

Threat A potential activity that would, if it occurred, exploit a vulnerability in a system.

Vulnerability A weakness in a system that may permit the realization of a threat.

Review Questions

1. An organization that needs to understand vulnerabilities and threats needs to perform a:
   a. Penetration test
   b. Business impact analysis
   c. Qualitative risk assessment
   d. Quantitative risk assessment
2. A risk manager has performed a risk analysis on a server that is worth $120,000. The risk manager has determined that the single loss expectancy is $100,000. The exposure factor is:
   a. 83%
   b. 1.2
   c. 80%
   d. 120%
3. A risk manager has performed a risk analysis on a server that is worth $120,000. The single loss expectancy (SLE) is $100,000, and the annual loss expectancy (ALE) is $8,000. The annual rate of occurrence (ARO) is:
   a. 12.5
   b. 92%
   c. 8
   d. 8%
4. A risk manager needs to implement countermeasures on a critical server. What factors should be considered when analyzing different solutions?
   a. Original annualized loss expectancy (ALE)
   b. Annualized loss expectancy (ALE) that results from the implementation of the countermeasure
   c. Original exposure factor (EF)
   d. Original single loss expectancy (SLE)
5. The general approaches to risk treatment are:
   a. Risk acceptance, risk avoidance, and risk reduction
   b. Risk acceptance, risk reduction, and risk transfer
   c. Risk acceptance, risk avoidance, risk reduction, and risk transfer
   d. Risk analysis, risk acceptance, risk reduction, and risk transfer

6. CIA refers to:
   a. Confidence, integrity, and audit of information and systems
   b. Confidentiality, integrity, and assessment of information and systems
   c. Confidentiality, integrity, and availability of information and systems
   d. Cryptography, integrity, and audit of information and systems
7. A recent failure in a firewall resulted in all incoming packets being blocked. This type of failure is known as:
   a. Fail open
   b. Access failure
   c. Circuit closed
   d. Fail closed
8. The definition of PII:
   a. Is name, date of birth, and home address
   b. Is name, date of birth, home address, and home telephone number
   c. Is name, date of birth, and social insurance number
   d. Varies by jurisdiction and regulation
9. The statement, "All financial transactions are to be encrypted using 3DES" is an example of a:
   a. Procedure
   b. Guideline
   c. Standard
   d. Policy
10. The purpose of information classification is:
    a. To establish procedures for safely disposing of information
    b. To establish procedures for the protection of information
    c. To establish procedures for information labeling
    d. To establish sensitivity levels for information
11. An organization is concerned that its employees will intentionally reveal its secrets to other parties. The organization should implement:
    a. Document marking
    b. Non-disclosure agreements
    c. Logon banners
    d. Security awareness training

12. The purpose of a background verification is to:
    a. Obtain independent verification of claims on an employment application
    b. Determine if the applicant should be hired
    c. Determine if the applicant is suitable for the job description
    d. Determine the applicant's honesty
13. When an employee is terminated from employment, the employee's access to computers should be terminated:
    a. At the next monthly audit
    b. At the next quarterly audit
    c. Within seven days
    d. Within one day
14. Security awareness training should be:
    a. Mandatory for information workers only
    b. Optional
    c. Provided at the time of hire and annually thereafter
    d. Provided at the time of hire
15. Management in an organization regularly reassigns employees to different functions. This practice is known as:
    a. Job rotation
    b. Reassignment
    c. Separation of duties
    d. Due diligence

Hands-On Projects

Project 1-1: Defense in Depth Network Design

In this project you will design a new network infrastructure for a five-hundred-employee law firm. The design of the network should incorporate several elements that demonstrate a defense in depth architecture.

The design of the network should incorporate protection against the following threats:

- Malicious software
- Phishing
- Spam
- Leakage of intellectual property

- Non-company-owned devices on the internal network ("bring your own device," or BYOD)
- Rogue access points

For each type of threat, indicate the controls or features in the architecture that reduce or eliminate the threat.

This project is not so much about network technology as it is about the concept of defense in depth. Do not worry about whether you have incorporated the latest or the most precisely correct technologies in your design.

Project 1-2: Data Sensitivity Procedures

In this project you will develop data sensitivity procedures.

1. Develop a matrix with three columns, one for each of three levels of increasing sensitivity. Choose easily understood titles for each level.
2. The rows of the matrix should consist of various data-handling activities including:
   - E-mail
   - Fax
   - Courier
   - Laptop computer
   - Hard copy
3. The cells of the matrix should specify whether the activity is permitted (for instance, if the most sensitive documents are permitted to be faxed) and, if so, under what conditions.
4. Opine on the matter of the number of sensitivity levels: how few or how many are needed, and how realistic is it to expect employees in an organization to be able to understand the classification levels and the procedures for protecting information at each level.

Project 1-3: Security Awareness Training

In this project you will develop an outline for a security awareness training plan for a thousand-employee company. You are to determine:

1. What training new employees should receive upon hire.
2. What written materials should be issued to new employees.
3. What materials should be available on an intranet site.
4. What types of security awareness messages should be issued to employees.

5. What specialized training should be available to IT personnel.
6. What recordkeeping for training should take place.

Case Projects

Case Project 1-1: Qualitative Risk Assessment

As a consultant with the Risk Analysis Consulting Co., you have been asked to perform a qualitative risk assessment for the TRC Chemical Company.

TRC Chemical has a large outside sales force, numbering in the hundreds. Most of these employees use their own home computers (70% laptops, 30% desktops) to conduct TRC Chemical business. You have been asked to assess the risks associated with the use of home computers versus company-owned and -managed computers.

Case Project 1-2: Quantitative Risk Assessment

As a consultant with the Risk Analysis Consulting Co., you have completed a qualitative risk assessment regarding the risks associated with using non-company-owned computers to conduct company business. Your customer, TRC Chemical, is pleased with the results of the qualitative risk assessment and wants to see hard numbers to see whether it can justify the capital and expense burden of equipping the sales force with company-owned computers, based upon risk mitigation alone.

In your risk assessment, make best estimates on the value of information and costs associated with purchasing and supporting company-owned computers.

Case Project 1-3: Segregation of Duties Matrix

As a consultant with the Risk Analysis Consulting Co., you have been asked to help the BBX Internet Stock Trading Company develop a viable segregation of duties for the management of its online software and supporting infrastructure.

The activities that BBX is concerned with include:

- Request and assignment of privileged access at the network, operating system, database, and application layers
- Setup of new customers
- Changes to audit alert settings

For each of the activities listed above, develop a segregation of duties matrix where different parts of each process are performed by different individuals. Things to consider:

- Separate the activity of requesting an action from performing the action.
- Add an activity of confirming correct completion of the action.
- Include any recordkeeping for the action so that an auditor can examine the action after the fact to see if the action was appropriately carried out.