C H A P T E R

1

✦   ✦   ✦   ✦

Security Management Practices

In our first chapter, we enter the domain of Security Management. Throughout this book, you will see that many Information Systems Security domains have several elements and concepts that overlap. Although all other security domains are clearly focused, this domain introduces concepts that we extensively touch upon in both the Operations Security (Chapter 6) and Physical Security (Chapter 10) domains. A CISSP professional will be expected to know the following:

✦ Basic security management concepts

✦ The difference between policies, standards, guidelines, and procedures

✦ Security awareness concepts

✦ Risk management (RM) practices

✦ Data classification levels

We will examine the InfoSec domain of Security Management by using the following elements:

✦ Concepts of Information Security Management

✦ The Information Classification process

✦ Security Policy implementation

✦ The roles and responsibilities of Security Administration

✦ Risk Management Assessment tools

✦ Security Awareness training

> **Note** Throughout the book we have footnotes that will help direct the reader to additional study sources.

Domain Definition

The InfoSec domain of Security Management incorporates the identification of information data assets with the development and implementation of policies, standards, guidelines, and procedures. It defines the management practices of data classification and risk management. It also addresses confidentiality, integrity, and availability by identifying threats, classifying the organization's assets, and rating their vulnerabilities so that effective security controls can be implemented.

Management Concepts

Under the heading of Information Security Management concepts, we will discuss the following:

✦ The big three: Confidentiality, Integrity, and Availability

✦ The concepts of identification, authentication, accountability, authorization, and privacy

✦ The objective of security controls (to reduce the impact of threats and the likelihood of their occurrence)

System Security Life Cycle

Security, like other aspects of an IT system, is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle, but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal.

Chapter 11 in the ISSEP study section describes systems security engineering in more detail, but let's get to know the basic steps of the system security life cycle. The order of these phases is*:

1. *Initiation phase*. During the initiation phase, the need for a system is expressed and the purpose of the system is documented.

2. *Development/acquisition phase*. During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed.

3. *Implementation phase*. During implementation, the system is tested and installed or fielded.

---

*Source: NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems."

4. *Operation/maintenance phase*. During this phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events.

5. *Disposal phase*. The disposal phase of the IT system life cycle involves the disposition of information, hardware, and software.

The Big Three

Throughout this book, you will read about the three tenets of InfoSec: Confidentiality, Integrity, and Availability (C.I.A.), as shown in Figure 1-1. These concepts represent the three fundamental principles of information security. All of the information security controls and safeguards and all of the threats, vulnerabilities, and security processes are subject to the C.I.A. yardstick.
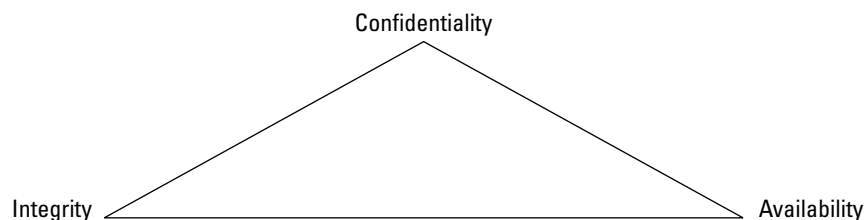
Figure 1-1: The C.I.A. triad.

Confidentiality. The concept of confidentiality attempts to prevent the intentional or unintentional unauthorized disclosure of a message's contents. Loss of confidentiality can occur in many ways, such as through the intentional release of private company information or through a misapplication of network rights.

Integrity. The concept of integrity ensures that:

- Modifications are not made to data by unauthorized personnel or processes

- Unauthorized modifications are not made to data by authorized personnel or processes

- The data is internally and externally consistent; in other words, that the internal information is consistent among all subentities and that the internal information is consistent with the real-world, external situation

Availability. The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate personnel. In other words, availability guarantees that the systems are up and running when needed. In addition, this concept guarantees that the security services that the security practitioner needs are in working order.

> **Note**   The reverse of confidentiality, integrity, and availability is disclosure, alteration, and destruction (D.A.D.).

Other Important Concepts

There are also several other important concepts and terms that a CISSP candidate must fully understand. These concepts include identification, authentication, accountability, authorization, and privacy, and are found frequently throughout the book:

Identification. The means by which users claim their identities to a system. Most commonly used for access control, identification is necessary for authentication and authorization.

Authentication. The testing or reconciliation of evidence of a user's identity. It establishes the user's identity and ensures that the users are who they say they are.

Accountability. A system's capability to determine the actions and behaviors of a single individual within a system and to identify that particular individual. Audit trails and logs support accountability.

Authorization. The rights and permissions granted to an individual or process that enable access to a computer resource. Once a user's identity and authentication are established, authorization levels determine the extent of system rights that a user can hold.

Privacy. The level of confidentiality and privacy protection given to a user in a system. This is often an important component of security controls. Privacy not only guarantees the fundamental tenet of confidentiality of a company's data, but also guarantees the data's level of privacy, which is being used by the operator.

NIST 33 Security Principles

In June 2001, the National Institute of Standards and Technology's (NIST) Information Technology Laboratory (ITL) published NIST Special Publication (SP) 800-27, "Engineering Principles for Information Technology Security (EP-ITS)" to assist in the secure design, development, deployment, and life cycle of information systems. It presents 33 security principles that start at the design phase of the information system or application and continue until the system's retirement and secure disposal. Some of the 33 principles that are most applicable to security management are*:

Principle 1. Establish a sound security policy as the foundation for design.

Principle 2. Treat security as an integral part of the overall system design.

---

*Source: NIST SP 800-27, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)," and "Federal Systems Level Guidance for Securing Information Systems," James Corrie, August 16, 2001.

Principle 5. Assume that external systems are insecure.

Principle 6. Identify potential trade-offs between reducing risk and increased costs and decreases in other aspects of operational effectiveness.

Principle 7. Implement layered security; ensure there is no single point of vulnerability (see sidebar).

Principle 11. Minimize the system elements to be trusted.

Principle 16. Isolate public access systems from mission critical resources (e.g., data, processes, etc.).

Principle 17. Use boundary mechanisms to separate computing systems and network infrastructures.

Principle 22. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.

Principle 23. Use unique identities to ensure accountability.

Principle 24. Implement least privilege.

Trade-Off Analysis (TOA)

▶ ISSEP

The simplest examples of a trade-off analysis are the choices we make every minute of every day, often subconsciously, weighing the pros and cons of any action and the benefit versus the cost of each decision. In security management, this cost versus benefit analysis is a very important process. The need for, or value of, a particular security control must be weighed against its impact or resource allocation drain and its usefulness. Any company can have exemplary security with an infinite budget, but there is always a point of diminishing returns, when the security demands interfere with the primary business. Making the financial case to upper management for various security controls is a very important part of a security manager's function.

Layered Security Architecture

Security designs should consider a layered approach to address or protect against a specific threat or to reduce vulnerability. For example, the use of a packet-filtering router in conjunction with an application gateway and an intrusion detection system combine to increase the work-factor an attacker must expend to successfully attack the system. The need for layered protections is important when commercial-off-the-shelf (COTS) products are used. The current state-of-the-art for security quality in COTS products does not provide a high degree of protection against sophisticated attacks. It is possible to help mitigate this situation by placing several controls in levels, requiring additional work by attackers to accomplish their goals.

(Source: NIST SP 800-27, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)")

A trade-off analysis can be formal or informal, depending upon the audience and the intent of the analysis. If the audience of the TOA is higher management or a client, often a formalized TOA, supported by objective evidence, documentation, and reports will be necessary. If the TOA is intended to be examined by internal staff or department, often it can be less formal. But the fundamental concepts and principles still apply in either case.

TOA Elements

The steps in a TOA are similar to the steps in the systems engineering methodology (see Chapter 11). The general steps in the TOA (formal or informal) are:

1. *Define the Objective*. The TOA is started by identifying the requirements that the solution must fulfill. These requirements can be expressed in terms of measures of effectiveness (MOEs).

2. *Identify Alternatives*. An effort must be made to identify the possible potential courses of action and include all promising candidate alternatives. Any course of action or possible candidate solution that fails to comply with any essential requirement should be rejected.

3. *Compare Alternatives*. The candidate solutions should be compared with one another with respect to each of the MOEs. The relative order of merit is judged by the cumulative rating of all the MOEs.

The detailed steps in a formal trade-off analysis process include:

1. Define the objectives.

2. Identify viable alternatives.

3. Define the selection criteria.

4. Assign weighing factors to selection criteria.

5. Assign value ratings for alternatives.

6. Calculate competitive scores.

7. Analyze the results.

8. Create the TOA report.

Objectives of Security Controls

The objective of security controls is to reduce vulnerabilities to a tolerable level and minimize the effect of an attack. To achieve this, the organization must determine the impact that an attack might have on an organization and the likelihood that the loss could occur. The process that analyzes various threat scenarios and produces a representative value for the estimated potential loss is constituted in the Risk Analysis (RA).

Controls function as countermeasures for vulnerabilities. There are many kinds, but generally they are categorized into four types*:

✦ *Deterrent controls* reduce the likelihood of a deliberate attack.

✦ *Preventative controls* protect vulnerabilities and make an attack unsuccessful or reduce its impact. Preventative controls inhibit attempts to violate security policy.

✦ *Corrective controls* reduce the effect of an attack.

✦ *Detective controls* discover attacks and trigger preventative or corrective controls. Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

To visualize the effect of security controls, it might help to create a matrix, wherein the y-axis represents the level of impact of a realized threat and the x-axis represents the likelihood of the threat being realized. When the matrix is created, it produces the graph shown in Figure 1-2. A properly implemented control should move the plotted point from the upper right — the threat value defined before the control was implemented — to the lower left (that is, toward 0,0) after the control is implemented. This concept is also useful when determining a control's cost/benefit ratio.
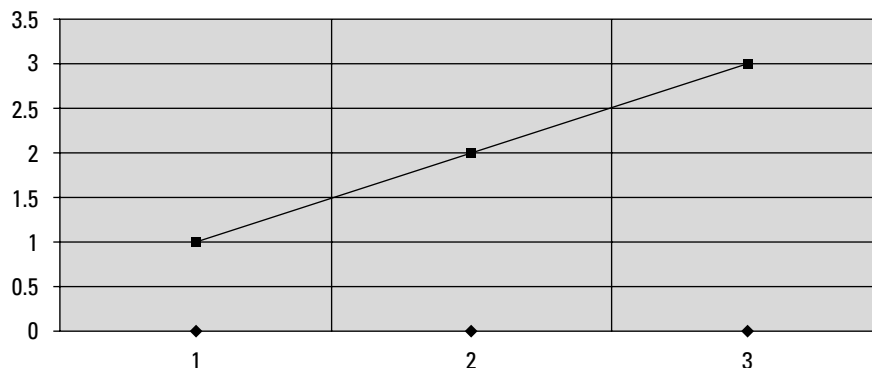
Figure 1-2: Simple threat matrix.

Therefore, an improperly designed or implemented control will show very little to no movement in the point before and after the control's implementation. The point's movement toward the 0,0 range could be so small (or in the case of badly designed controls, in the opposite direction) that it does not warrant the expense of implementation.

*Source: *Introduction to Risk Analysis*, C & A Security Risk Analysis Group and NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems."

OMB Circular A-130

The Office of Management and Budget Circular A-130, revised November 30, 2000, requires that a review of the security controls for each major government application be performed at least every three years. For general support systems, OMB Circular A-130 requires that the security controls either be reviewed by an independent audit or self review. Audits can be self-administered or independent (either internal or external). The essential difference between a self-audit and an independent audit is objectivity; however, some systems may require a fully independent review. More information on auditing can be found in Chapter 6.

The goal, the 0,0 point (no threat with no likelihood), is obviously impossible to achieve because a very unlikely threat could still exist and have some measurable impact. For example, the possibility that a flaming pizza delivery van will crash into the operations center is extremely unlikely; however, this situation would likely have a fairly serious impact on the availability of computing resources.

Information Classification Process

The first major process that we examine in this chapter is the concept of Information Classification. The Information Classification process is related to the domain of Business Continuity Planning and Disaster Recovery Planning because both focus on business risk and data valuation, yet it is still a fundamental concept in its own right — one that a CISSP candidate must understand.

Information Classification Objectives

There are several good reasons to classify information. Not all data has the same value to an organization. Some data is more valuable to the people who are making strategic decisions because it aids them in making long-range or short-range business direction decisions. Some data, such as trade secrets, formulas, and new product information, is so valuable that its loss could create a significant problem for the enterprise in the marketplace by creating public embarrassment or by causing a lack of credibility.

For these reasons, it is obvious that information classification has a higher, enterprise-level benefit. Information can have an impact on a business globally, not just on the business unit or line operation levels. Its primary purpose is to enhance confidentiality, integrity, and availability and to minimize the risks to the information. In addition, by focusing the protection mechanisms and controls on the information areas that need it the most, you achieve a more efficient cost-to-benefit ratio.

Information classification has the longest history in the government sector. Its value has long been established, and it is a required component when securing trusted

systems. In this sector, information classification is used primarily to prevent the unauthorized disclosure of information and the resultant failure of confidentiality.

You can also use information classification to comply with privacy laws or to enable regulatory compliance. A company might wish to employ classification to maintain a competitive edge in a tough marketplace. There might also be sound legal reasons for a company to employ information classification, such as to minimize liability or to protect valuable business information.

Information Classification Benefits

In addition to the reasons mentioned previously, employing information classification has several clear benefits to an organization. Some of these benefits are as follows:

✦ Demonstrates an organization's commitment to security protections

✦ Helps identify which information is the most sensitive or vital to an organization

✦ Supports the tenets of confidentiality, integrity, and availability as it pertains to data

✦ Helps identify which protections apply to which information

✦ Might be required for regulatory, compliance, or legal reasons

Information Classification Concepts

The information that an organization produces or processes must be classified according to the organization's sensitivity to its loss or disclosure. These data owners are responsible for defining the sensitivity level of the data. This approach enables the security controls to be properly implemented according to the classification scheme.

Classification Terms

The following definitions describe several governmental data classification levels ranging from the lowest level of sensitivity to the highest:

1. *Unclassified.* Information designated as neither sensitive nor classified. The public release of this information does not violate confidentiality.

2. *Sensitive but Unclassified (SBU).* Information designated as a minor secret but might not create serious damage if disclosed. Answers to tests are an example of this kind of information. Health care information is another example of SBU data.

3. *Confidential.* Information designated to be of a confidential nature. The unauthorized disclosure of this information could cause some damage to the country's national security. This level applies to documents labeled between SBU and Secret in sensitivity.

4. *Secret.* Information designated of a secret nature. The unauthorized disclosure of this information could cause serious damage to the country's national security.

5. *Top Secret.* The highest level of information classification. The unauthorized disclosure of Top Secret information will cause exceptionally grave damage to the country's national security.

In all of these categories, in addition to having the appropriate clearance to access the information, an individual or process must have a "need to know" the information. Thus, an individual cleared for Secret or below is not authorized to access Secret material that is not needed for him or her to perform assigned job functions.

In addition, the following classification terms are also used in the private sector (see Table 1-1):

1. *Public.* Information that is similar to unclassified information; all of a company's information that does not fit into any of the next categories can be considered public. While its unauthorized disclosure may be against policy, it is not expected to impact seriously or adversely the organization, its employees, and/or its customers.

2. *Sensitive.* Information that requires a higher level of classification than normal data. This information is protected from a loss of confidentiality as well as from a loss of integrity due to an unauthorized alteration. This classification applies to information that requires special precautions to assure the integrity of the information by protecting it from unauthorized modification or deletion. It is information that requires a higher-than-normal assurance of accuracy and completeness.

3. *Private.* This classification applies to personal information that is intended for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization and/or its employees. For example, salary levels and medical information are considered private.

4. *Confidential.* This classification applies to the most sensitive business information that is intended strictly for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization, its stockholders, its business partners, and/or its customers. This information is exempt from disclosure under the provisions of the Freedom of Information Act or other applicable federal laws or regulations. For example, information about new product development, trade secrets, and merger negotiations is considered confidential.

An organization may use the high, medium, or low classification scheme based upon its C.I.A. needs and whether it requires high, medium, or low protective controls. For example, a system and its information may require a high degree of integrity and availability, yet have no need for confidentiality.

Table 1-1
Private/Commercial Sector Information Classification Scheme

Definition	*Description*
Public Use	Information that is safe to disclose publicly
Internal Use Only	Information that is safe to disclose internally but not externally
Company Confidential	The most sensitive need-to-know information

The designated owners of information are responsible for determining data classification levels, subject to executive management review. Table 1-2 shows a simple H/M/L data classification for sensitive information.

Table 1-2
H/M/L Data Classification

Category	*Description*
High	Could cause loss of life, imprisonment, major financial loss, or require legal remediation if the information is compromised.
Medium	Could cause noticeable financial loss if the information is compromised.
Low	Would cause only minor financial loss or require minor administrative action for correction if the information is compromised

(Source: NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems.")

Classification Criteria

Several criteria may be used to determine the classification of an information object:

Value. Value is the number one commonly used criteria for classifying data in the private sector. If the information is valuable to an organization or its competitors, it needs to be classified.

Age. The classification of information might be lowered if the information's value decreases over time. In the Department of Defense, some classified documents are automatically declassified after a predetermined time period has passed.

Useful Life. If the information has been made obsolete due to new information, substantial changes in the company, or other reasons, the information can often be declassified.

Personal Association. If information is personally associated with specific individuals or is addressed by a privacy law, it might need to be classified. For example, investigative information that reveals informant names might need to remain classified.

Information Classification Procedures

There are several steps in establishing a classification system. These are the steps in priority order:

1. Identify the administrator and data custodian.

2. Specify the criteria for classifying and labeling the information.

3. Classify the data by its owner, who is subject to review by a supervisor.

4. Specify and document any exceptions to the classification policy.

5. Specify the controls that will be applied to each classification level.

6. Specify the termination procedures for declassifying the information or for transferring custody of the information to another entity.

7. Create an enterprise awareness program about the classification controls.

Distribution of Classified Information

External distribution of classified information is often necessary, and the inherent security vulnerabilities will need to be addressed. Some of the instances when this distribution is necessary are as follows:

Court order. Classified information might need to be disclosed to comply with a court order.

Government contracts. Government contractors might need to disclose classified information in accordance with (IAW) the procurement agreements that are related to a government project.

Senior-level approval. A senior-level executive might authorize the release of classified information to external entities or organizations. This release might require the signing of a confidentiality agreement by the external party.

Information Classification Roles

The roles and responsibilities of all participants in the information classification program must be clearly defined. A key element of the classification scheme is the role that the users, owners, or custodians of the data play in regard to the data. These roles are important to remember.

Various officials and organizational offices are typically involved with computer security. They include the following groups:

- ✦ Senior management
- ✦ Program managers
- ✦ Application owners
- ✦ Computer security management
- ✦ Technology providers
- ✦ Supporting organizations
- ✦ Users

Senior management has the final responsibility through due care and due diligence to preserve the capital of the organization and further its business model through the implementation of a security program. While senior management does not have the functional role of managing security procedures, it has the ultimate responsibility to see that business continuity is preserved.

Owner

An information owner might be an executive or manager of an organization. This person is responsible for the information assets that must be protected. An owner is different from a custodian. The owner has the final corporate responsibility of data protection, and under the concept of due care the owner might be liable for negligence because of the failure to protect this data. The actual day-to-day function of protecting the data, however, belongs to a custodian.

The responsibilities of an information owner could include the following:

- ✦ Making the original decision about what level of classification the information requires, which is based upon the business needs for the protection of the data
- ✦ Reviewing the classification assignments periodically and making alterations as the business needs change
- ✦ Delegating the responsibility of the data protection duties to the custodian

The information owner for information stored within, processed by, or transmitted by a system may or may not be the same as the System Owner. Also, a single system may utilize information from multiple Information Owners. The Information Owner is responsible for establishing the rules for appropriate use and protection of the subject data/information (rules of behavior). The Information Owner retains that responsibility even when the data/information are shared with other organizations.*

---

*Source: NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems."

The System Owner is responsible for ensuring that the security plan is prepared and for implementing the plan and monitoring its effectiveness. The System Owner is responsible for defining the system's operating parameters, authorized functions, and security requirements.

Custodian

The owner of information delegates the responsibility of protecting that information to the information custodian. IT systems personnel commonly execute this role. The duties of a custodian might include the following:

✦ Running regular backups and routinely testing the validity of the backup data

✦ Performing data restoration from the backups when necessary

✦ Maintaining those retained records IAW the established information classification policy

The custodian might also have additional duties, such as being the administrator of the classification scheme.

User

In the information classification scheme, an end user is considered to be anyone (such as an operator, employee, or external party) who routinely uses the information as part of his or her job. This person can also be considered a consumer of the data — someone who needs daily access to the information to execute tasks. The following are a few important points to note about end users:

✦ Users must follow the operating procedures defined in an organization's security policy, and they must adhere to the published guidelines for its use.

✦ Users must take "due care" to preserve the information's security during their work (as outlined in the corporate information use policies). They must prevent "open view" from occurring (see sidebar).

✦ Users must use company computing resources only for company purposes and not for personal use.

Organizations should ensure an effective administration of users' computer access to maintain system security, including user account management, auditing, and the timely modification or removal of system access.* This includes:

User Account Management. Organizations should have a process for requesting, establishing, issuing, and closing user accounts, tracking users and their respective access authorizations, and managing these functions.

---

*Source: NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems."

Management Reviews. It is necessary to periodically review user accounts. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, and whether required training has been completed.

Detecting Unauthorized/Illegal Activities. Mechanisms besides auditing and analysis of audit trails should be used to detect unauthorized and illegal acts, such as rotating employees in sensitive positions, which could expose a scam that required an employee's presence, or periodic re-screening of personnel.

Employee Termination

Although actually under the purview of Human Resources, it's important that the ISO understand the impact of employee terminations on the integrity of the computer systems. Normally there are two types of terminations, friendly and unfriendly, and both require specific actions.

Friendly terminations should be accomplished by implementing a standard set of procedures for outgoing or transferring employees.* This normally includes:

✦ The removal of access privileges, computer accounts, authentication tokens.

✦ The briefing on the continuing responsibilities for confidentiality and privacy.

✦ The return of company computing property, such as laptops.

✦ The continued availability of data. In both the manual and the electronic worlds this may involve documenting procedures or filing schemes, such as how documents are stored on the hard disk and how they are backed up. Employees should be instructed whether or not to "clean up" their PC before leaving.

✦ If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured.

Given the potential for adverse consequences during an unfriendly termination, organizations should do the following:

✦ System access should be terminated as quickly as possible when an employee is leaving a position under less-than-friendly terms. If employees are to be fired, system access should be removed at the same time (or just before) the employees are notified of their dismissal.

✦ When an employee notifies an organization of the resignation and it can be reasonably expected that it is on unfriendly terms, system access should be immediately terminated, or as soon as is feasible.

*Source: NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems."

Open View

The term *open view* refers to the act of leaving classified documents in the open where an unauthorized person can see them, thus violating the information's confidentiality. Procedures to prevent open view should specify that information is to be stored in locked areas or transported in properly sealed containers, for example.

✦ During the *notice of termination* period, it may be necessary to assign the individual to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications.

✦ In some cases, physical removal from the offices may be necessary.

In either scenario, network access and system rights must be strictly controlled.

Security Policy Implementation

Security policies are the foundation of a sound security implementation. Often organizations will implement technical security solutions without first creating this foundation of policies, standards, guidelines, and procedures, unintentionally creating unfocused and ineffective security controls.

We discuss the following questions in this section:

✦ What are policies, standards, guidelines, and procedures?

✦ Why do we use policies, standards, guidelines, and procedures?

✦ What are the common policy types?

Policies, Standards, Guidelines, and Procedures

A policy is one of those terms that can mean several things. For example, there are security policies on firewalls, which refer to the access control and routing list information. Standards, procedures, and guidelines are also referred to as policies in the larger sense of a global information security policy.

A good, well-written policy is more than an exercise created on white paper — it is an essential and fundamental element of sound security practice. A policy, for example, can literally be a lifesaver during a disaster, or it might be a requirement of a governmental or regulatory function. A policy can also provide protection from liability due to an employee's actions, or it can control access to trade secrets.

NIST categorizes computer system security policies into three basic types:

✦ *Program policy* — used to create an organization's computer security program

✦ *Issue-specific policies* — used to address specific issues of concern to the organization

✦ *System-specific policies* — technical directives taken by management to protect a particular system

Program policies and issue-specific policies both address policy from a broad level, usually encompassing the entire organization. Program policy is traditionally more general and strategic; for example, the organization's overall computer security program may be defined in a program policy. An issue-specific policy is a nontechnical policy addressing a single or specific issue of concern to the organization, such as the procedural guidelines for checking disks brought to work or email privacy concerns. Issue-specific policies are similar to program policies, in that they are not technically focused.

However, program policy and issue-specific policies do not provide sufficient information or direction, for example, to be used in establishing an access control list or in training users on what actions are permitted. System-specific policies fill this need. A system-specific policy is technically focused and addresses only one computer system or device type.

Table 1-3 helps illustrate the difference between these three types of NIST policies.

Table 1-3
NIST Security Policy Types

| Policy Type	Description	Example
Program policy	High-level program policy	Senior-level management statement
Issue-specific policy	Addresses single issue	Email privacy policy
System-specific policy	Single-system directives	Router access control lists

(Source: National Institute of Standards and Technology, "An Introduction to Computer Security: The NIST Handbook Special Publication 800-12.")

Policy Types

In the corporate world, when we refer to specific polices rather than a group policy, we generally refer to those policies that are distinct from the standards, procedures, and guidelines. As you can see from the policy hierarchy chart in Figure 1-3, policies are considered the first and highest level of documentation, from which the

lower level elements of standards, procedures, and guidelines flow. This order, how-
ever, does not mean that policies are more important than the lower elements.
These higher-level policies, which are the more general policies and statements,
should be created first in the process for strategic reasons, and then the more tacti-
cal elements can follow.
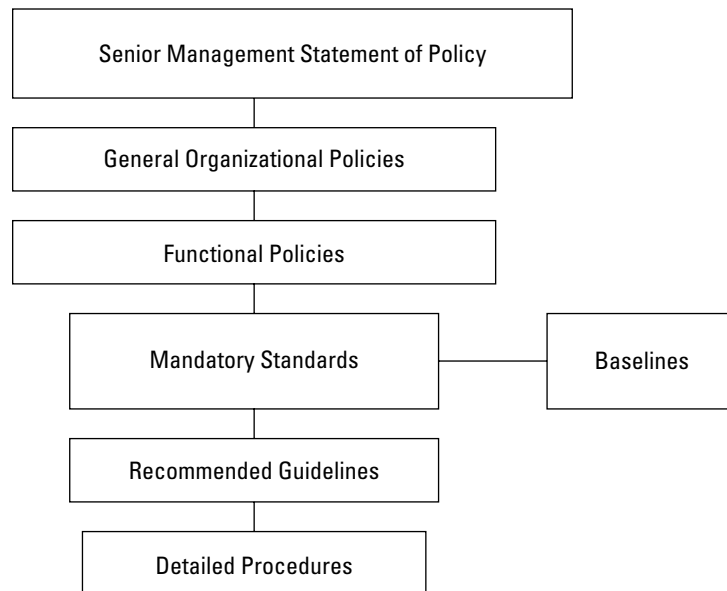
Figure 1-3: Security Policy Hierarchy.

Senior Management Statement of Policy. The first policy of any policy cre-
ation process is the Senior Management Statement of Policy. This is a general,
high-level statement of a policy that contains the following elements:

- An acknowledgment of the importance of the computing resources to
  the business model
- A statement of support for information security throughout the enterprise
- A commitment to authorize and manage the definition of the lower-level
  standards, procedures, and guidelines

Regulatory. Regulatory policies are security policies that an organization
must implement due to compliance, regulation, or other legal requirements.
These companies might be financial institutions, public utilities, or some
other type of organization that operates in the public interest. These policies
are usually very detailed and are specific to the industry in which the organi-
zation operates.

Regulatory polices commonly have two main purposes:

1. To ensure that an organization is following the standard procedures or base practices of operation in its specific industry

2. To give an organization the confidence that it is following the standard and accepted industry policy

Advisory. Advisory policies are security polices that are not mandated to be followed but are strongly suggested, perhaps with serious consequences defined for failure to follow them (such as termination, a job action warning, and so forth). A company with such policies wants most employees to consider these policies mandatory. Most policies fall under this broad category.

Advisory policies can have many exclusions or application levels. Thus, these policies can control some employees more than others, according to their roles and responsibilities within that organization. For example, a policy that requires a certain procedure for transaction processing might allow for an alternative procedure under certain, specified conditions.

Informative. Informative policies are policies that exist simply to inform the reader. There are no implied or specified requirements, and the audience for this information could be certain internal (within the organization) or external parties. This does not mean that the policies are authorized for public consumption but that they are general enough to be distributed to external parties (vendors accessing an extranet, for example) without a loss of confidentiality.

Especially high visibility should be afforded the formal issuance of security policy. This is because nearly all employees at all levels will in some way be affected, major organizational resources will be addressed, and many new terms, procedures, and activities will be introduced.

Including security as a regular topic at staff meetings at all levels of the organization can be helpful. Also, providing visibility through such avenues as management presentations, panel discussions, guest speakers, question/answer forums, and newsletters can be beneficial.

Senior Management Commitment

Fundamentally important to any security program's success is the senior management's high-level statement of commitment to the information security policy process and the senior management's understanding of how important security controls and protections are to the enterprise's continuity. Senior management must be aware of the importance of security implementation to preserve the organization's viability (and for their own "due care" protection) and must publicly support that process throughout the enterprise.

Standards, Guidelines, and Procedures

The next level down from policies is the three elements of policy implementation: standards, guidelines, and procedures. These three elements contain the actual details of the policy, such as how it should be implemented and what standards and procedures should be used. They are published throughout the organization via manuals, the intranet, handbooks, or awareness classes.

It is important to know that standards, guidelines, and procedures are separate yet linked documents from the general polices (especially the senior-level statement). Unfortunately, companies will often create one document that satisfies the needs of all of these elements. This situation is not good. There are a few good reasons why they should be kept separate:

✦ Each of these elements serves a different function and focuses on a different audience. Also, physical distribution of the policies is easier.

✦ Security controls for confidentiality are different for each policy type. For example, a high-level security statement might need to be available to investors, but the procedures for changing passwords should not be available to anyone who is not authorized to perform the task.

✦ Updating and maintaining the policy is much more difficult when all the policies are combined into one voluminous document. Mergers, routine maintenance, and infrastructure changes all require that the policies be routinely updated. A modular approach to a policy document will keep the revision time and costs down.

Standards. Standards specify the use of specific technologies in a uniform way. This standardization of operating procedures can be a benefit to an organization by specifying the uniform methodologies to be used for the security controls. Standards are usually compulsory and are implemented throughout an organization for uniformity.

Guidelines. Guidelines are similar to standards; they refer to the methodologies of securing systems, but they are only recommended actions and are not compulsory. Guidelines are more flexible than standards and take into consideration the varying nature of the information systems. Guidelines can be used to specify the way standards should be developed, for example, or to guarantee the adherence to general security principles.

Procedures. Procedures embody the detailed steps that are followed to perform a specific task. Procedures are the detailed actions that personnel must follow. They are considered the lowest level in the policy chain. Their purpose is to provide detailed steps for implementing the policies, standards, and guidelines previously created. *Practices* is also a term that is frequently used in reference to procedures.

Baselines. Once a consistent set of baselines has been created, we can design the security architecture of an organization and develop standards. Baselines take into consideration the difference between various operating systems, for example, to ensure that the security is being uniformly implemented throughout the enterprise.

Roles and Responsibilities

Although members of an organization frequently wear multiple hats, defined roles and responsibilities are important in the security administration process. Also, roles and responsibilities are central to the *separation of duties* concept — the concept that security is enhanced through the division of responsibilities in the production cycle. Therefore, it is important that individual roles and responsibilities are clearly communicated and understood (see Table 1-4).

Table 1-4 **Roles and Responsibilities**	
Role	*Description*
Senior Manager	Has the ultimate responsibility for security
InfoSec Officer	Has the functional responsibility for security
Owner	Determines the data classification
Custodian	Preserves the information's CIA
User/Operator	Performs IAW the stated policies
Auditor	Examines security

Some of these roles are:

> **Senior Management.** Executive or senior-level management is assigned the overall responsibility for the security of information. Senior management might delegate the function of security, but they are viewed as the end of the food chain when liability is concerned.
>
> **Information Systems Security Professionals.** Information systems security professionals are delegated the responsibility for implementing and maintaining security by the senior-level management. Their duties include the design, implementation, management, and review of the organization's security policy, standards, guidelines, and procedures.
>
> **Data Owners.** As we previously discussed in the section titled "Information Classification Roles," data owners are primarily responsible for determining the data's sensitivity or classification levels. They can also be responsible for maintaining the information's accuracy and integrity.
>
> **Users.** As we previously discussed in the section titled "Information Classification Roles," users are responsible for following the procedures set out in the organization's security policy during the course of their normal daily tasks.

Information Systems Auditors. Information systems auditors are responsible for providing reports to the senior management on the effectiveness of the security controls by conducting regular, independent audits. They also examine whether the security policies, standards, guidelines, and procedures effectively comply with the company's stated security objectives.

Risk Management

A major component of InfoSec is Risk Management (RM). RM's main function is to mitigate risk. Mitigating risk means to reduce risk until it reaches a level that is acceptable to an organization. We can define RM as the identification, analysis, control, and minimization of loss that is associated with events.

The identification of risk to an organization entails defining the following basic elements:

   ✦ The actual threat

   ✦ The possible consequences of the realized threat

   ✦ The probable frequency of the occurrence of a threat

   ✦ The extent of how confident we are that the threat will happen

Many formulas and processes are designed to help provide some certainty when answering these questions. We should point out, however, that because life and nature are constantly evolving and changing, we cannot consider every possibility. RM tries as much as possible to see the future and to lower the possibility of threats impacting a company.

Note   It's important to remember that the risk to an enterprise can never be totally eliminated; that would entail ceasing operations. Risk management means finding out what level of risk the enterprise can safely tolerate and still continue to function effectively.

Principles of Risk Management

The RM task process has several elements, primarily including the following:

   ✦ Performing a Risk Analysis, including the cost-benefit analysis of protections

   ✦ Implementing, reviewing, and maintaining protections

To enable this process, you will need to determine some properties of the various elements, such as the value of assets, threats, and vulnerabilities and the likelihood of events. A primary part of the RM process is assigning values to threats and estimating how often (or how likely) that threat will occur. To perform this task, several

formulas and terms have been developed, and the CISSP candidate must fully understand them. The terms and definitions listed in the following section are ranked in the order that they are defined during the Risk Analysis (RA).

The Purpose of Risk Analysis

The main purpose of performing a Risk Analysis is to quantify the impact of potential threats — to put a price or value on the cost of a lost business functionality. The two main results of an RA — the identification of risks and the cost/benefit justification of the countermeasures — are vitally important to the creation of a risk mitigation strategy.

There are several benefits to performing an RA. It creates a clear cost-to-value ratio for security protections. It also influences the decision-making process dealing with hardware configuration and software systems design. In addition, it helps a company focus its security resources where they are needed most. Furthermore, it can influence planning and construction decisions, such as site selection and building design.

Terms and Definitions

The following are RA terms that the CISSP candidate will need to know:

Asset. An asset is a resource, process, product, computing infrastructure, and so forth that an organization has determined must be protected. The loss of the asset could intangibly affect confidentiality, integrity, or availability, or it could have a tangible dollar value. It could also affect the ability of an organization to continue in business. The value of an asset is composed of all of the elements that are related to that asset — its creation, development, support, replacement, public credibility, considered costs, and ownership values.

Threat. Simply put, the presence of any potential event that causes an undesirable impact on the organization is called a threat. As we will discuss in the Operations Domain, a threat could be man-made or natural and could have a small or large effect on a company's security or viability.

Vulnerability. The absence or weakness of a safeguard constitutes a vulnerability. A minor threat has the potential to become a greater or more frequent threat because of a vulnerability. Think of a vulnerability as the threat that gets through a safeguard into the system. Combined with the terms asset and threat, vulnerability is the third part of an element that is called a *triple* in risk management.

Safeguard. A safeguard is the control or countermeasure employed to reduce the risk associated with a specific threat or group of threats.

Exposure Factor (EF). The EF represents the percentage of loss that a realized threat event would have on a specific asset. This value is necessary to compute the Single Loss Expectancy (SLE), which in turn is necessary to compute the Annualized Loss Expectancy (ALE). The EF can be a small percentage, such as the effect of a loss of some hardware, or a very large percentage, such as the catastrophic loss of all computing resources.

Single Loss Expectancy (SLE). An SLE is the dollar figure that is assigned to a single event. It represents an organization's loss from a single threat and is derived from the following formula:

Asset Value (\$) $\times$ Exposure Factor (EF) = SLE

For example, an asset valued at \$100,000 that is subjected to an exposure factor of 30 percent would yield an SLE of \$30,000. While this figure is defined primarily in order to create the Annualized Loss Expectancy (ALE), it is occasionally used by itself to describe a disastrous event for a Business Impact Assessment (BIA).

Annualized Rate of Occurrence (ARO). The ARO is a number that represents the estimated frequency with which a threat is expected to occur. The range for this value can be from 0.0 (never) to a large number (for minor errors, such as misspellings of names in data entry). How this number is derived can be very complicated. It is usually created based upon the likelihood of the event and the number of employees that could make that error occur. The loss incurred by this event is not a concern here, only how often it occurs.

For example, a meteorite damaging the data center could be estimated to occur only once every 100,000 years and will have an ARO of .00001. In contrast, 100 data entry operators attempting an unauthorized access attempt could be estimated at six times a year per operator and will have an ARO of 600.

Annualized Loss Expectancy (ALE). The ALE, a dollar value, is derived from the following formula:

Single Loss Expectancy (SLE) $\times$ Annualized Rate of Occurrence (ARO) = ALE

In other words, an ALE is the annually expected financial loss to an organization from a threat. For example, a threat with a dollar value of \$100,000 (SLE) that is expected to happen only once in 1,000 years (ARO of .001) will result in an ALE of \$100. This example helps to provide a more reliable cost-benefit analysis. Remember that the SLE is derived from the asset value and the Exposure Factor (EF). Table 1-5 shows these formulas.

Table 1-5
Risk Analysis Formulas

Concept	*Derivation Formula*
Exposure Factor (EF)	Percentage of asset loss caused by threat
Single Loss Expectancy (SLE)	Asset Value x Exposure Factor (EF)
Annualized Rate of Occurrence (ARO)	Frequency of threat occurrence per year
Annualized Loss Expectancy (ALE)	Single Loss Expectancy (SLE) x Annualized Rate of Occurrence (ARO)

Overview of Risk Analysis

We now discuss the four basic elements of the Risk Analysis process:

1. Quantitative Risk Analysis

2. Qualitative Risk Analysis

3. Asset Valuation Process

4. Safeguard Selection

Quantitative Risk Analysis

The difference between quantitative and qualitative RA is fairly simple: Quantitative RA attempts to assign independently objective numeric values (hard dollars, for example) to the components of the risk assessment and to the assessment of potential losses. Qualitative RA addresses more intangible values of a data loss and focuses on other issues, rather than on the pure, hard costs.

When all elements (asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty, and probability) are measured, rated, and assigned values, the process is considered to be fully quantitative. Fully quantitative risk analysis is not possible, however, because qualitative measures must always be applied. Thus, you should be aware that just because the figures look hard on paper does not mean it is possible to foretell the future with any certainty.

A quantitative risk analysis process is a major project, and as such it requires a project or program manager to manage the main elements of the analysis. A major part of the initial planning for the quantitative RA is the estimation of the time required to perform the analysis. In addition, you must also create a detailed process plan and assign roles to the RA team.

A Preliminary Security Examination (PSE) is often conducted before the actual quantitative RA. The PSE helps to gather the elements that you will need when the actual RA takes place. A PSE also helps to focus an RA. Elements that are defined during this phase include asset costs and values, a listing of various threats to an organization (in terms of threats to both the personnel and the environment), and documentation of the existing security measures. The PSE is normally then subject to a review by an organization's management before the RA begins.

Any combination of the following techniques can be used in gathering information relevant to the IT system within its operational boundary*:

Questionnaire. The questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting the IT system.

---

*Source: NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems."

On-Site Interviews. On-site visits also allow risk assessment personnel to observe and gather information about the physical, environmental, and operational security of the IT system.

Document Review. Policy documents, system documentation, and security-related documentation can provide good information about the security controls used by and planned for the IT system.

Automated Scanning Tools. Proactive technical methods can be used to collect system information efficiently.

Risk Analysis Steps

The three primary steps in performing a risk analysis are similar to the steps in performing a Business Impact Assessment (see Chapter 8). A risk analysis is commonly much more comprehensive, however, and is designed to be used to quantify complicated, multiple-risk scenarios.

The three primary steps are as follows:

1. Estimate the potential losses to assets by determining their value.

2. Analyze potential threats to the assets.

3. Define the Annualized Loss Expectancy (ALE).

Estimate Potential Losses

To estimate the potential losses incurred during the realization of a threat, the assets must be valued by commonly using some sort of standard asset valuation process (we describe this task in more detail later). This process results in an assignment of an asset's financial value by performing the EF and the SLE calculations.

Analyze Potential Threats

Here, we determine what the threats are and how likely and often they are to occur. To define the threats, we must also understand the asset's vulnerabilities and perform an ARO calculation for the threat and vulnerabilities.

Automated Risk Analysis Products

There are several good automated risk analysis products on the market. The main objective of these products is to minimize the manual effort expended to create the risk analysis and to provide the capability to forecast expected losses quickly and with differing input variations. The creation of a database during an initial automated process enables the operator to rerun the analysis by using different parameters to create a what-if scenario. These products enable the users to perform calculations quickly in order to estimate future expected losses, thereby determining the benefit of their implemented safeguards.

All types of threats should be considered in this section, no matter whether they seem likely or not. It might be helpful to organize the threat listing into the types of threats by source or by their expected magnitude. In fact, some organizations can provide statistics on the frequency of various threats that occur in your area. In addition, the other domains of InfoSec discussed in this book have several varied listings of the categories of threats.

Some of the following categories of threats could be included in this section:

Data Classification. Data aggregation or concentration that results in data inference, covert channel manipulation, a malicious code/virus/Trojan horse/worm/logic bomb, or a concentration of responsibilities (lack of separation of duties).

Information Warfare. Technology-oriented terrorism, malicious code or logic, or emanation interception for military or economic espionage.

Personnel. Unauthorized or uncontrolled system access, misuse of technology by authorized users, tampering by disgruntled employees, or falsified data input.

Application/Operational. An ineffective security application that results in procedural errors or incorrect data entry.

Criminal. Physical destruction or vandalism, the theft of assets or information, organized insider theft, armed robbery, or physical harm to personnel.

Environmental. Utility failure, service outage, natural disasters, or neighboring hazards.

Computer Infrastructure. Hardware/equipment failure, program errors, operating system flaws, or a communications system failure.

Delayed Processing. Reduced productivity or a delayed funds collection that results in reduced income, increased expenses, or late charges.

Define the Annualized Loss Expectancy (ALE)
Once we have determined the SLE and ARO, we can estimate the ALE by using the formula that we previously described.

Results
After performing the Risk Analysis, the final results should contain the following:

✦ Valuations of the critical assets in hard costs

✦ A detailed listing of significant threats

✦ Each threat's likelihood and possible occurrence rate

✦ Loss potential by a threat — the dollar impact that the threat will have on an asset

✦ Recommended remedial measures and safeguards or countermeasures

Remedies

There are three generic remedies to risk that might take the form of either one or a combination of the following three:

> **Risk Reduction.** Taking measures to alter or improve the risk position of an asset throughout the company
>
> **Risk Transference.** Assigning or transferring the potential cost of a loss to another party (like an insurance company)
>
> **Risk Acceptance.** Accepting the level of loss that will occur and absorbing that loss

The remedy chosen will usually be the one that results in the greatest risk reduction while retaining the lowest annual cost necessary to maintain a company.

Qualitative Risk Analysis

As we mentioned previously, a qualitative RA does not attempt to assign hard and fast costs to the elements of the loss. It is more scenario-oriented, and as opposed to a quantitative RA, a purely qualitative risk analysis is possible. Threat frequency and impact data are required to do a qualitative RA, however.

In a qualitative risk assessment, the seriousness of threats and the relative sensitivity of the assets are given a ranking, or qualitative grading, by using a scenario approach and creating an exposure rating scale for each scenario.

During a scenario description, we match various threats to identified assets. A scenario describes the type of threat and the assets facing potential loss and selects safeguards to mitigate the risk.

Qualitative Scenario Procedure

After the threat listing has been created, the assets for protection have been defined, and an exposure level rating is assigned, the qualitative risk assessment scenario begins. See Table 1-6 for a simple exposure rating scale.

Table 1-6
Simple Exposure Rating Level Scale

Rating Level	*Exposure Percentage*
Blank or 0	No measurable loss
1	20% loss
2	40% loss
3	60% loss
4	80% loss
5	100% loss

The procedures in performing the scenario are as follows:

✦ A scenario is written that addresses each major threat.

✦ The business unit managers review the scenario for a reality check.

✦ The RA team recommends and evaluates the various safeguards for each threat.

✦ The RA team works through each finalized scenario by using a threat, asset, and safeguard.

✦ The team prepares their findings and submits them to management.

After the scenarios have all been played out and the findings are published, management must implement the safeguards that were selected as being acceptable and begin to seek alternatives for the safeguards that did not work.

Asset Valuation Process

There are several elements of a process that determine the value of an asset. Both quantitative and qualitative RA (and Business Impact Assessment) procedures require a valuation to be made of the asset's worth to the organization. This valuation is a fundamental step in all security auditing methodologies. A common universal mistake made by organizations is not accurately identifying the information's value before implementing the security controls. This situation often results in a control that is ill suited for asset protection, is not financially effective, or is protective of the wrong asset. Table 1-7 demonstrates quantitative versus qualitative RA.

Table 1-7
Quantitative versus Qualitative RA

Property	Quantitative	Qualitative
Cost/benefit analysis	Yes	No
Financial hard costs	Yes	No
Can be automated	Yes	No
Guesswork involved	Low	High
Complex calculations	Yes	No
Volume of information required	High	Low
Time/work involved	High	Low
Ease of communication	High	Low

Reasons for Determining the Value of an Asset

Here are some additional reasons to define the cost or value that we previously described:

✦ The asset valuation is necessary to perform the cost-benefit analysis.

✦ The asset's value might be necessary for insurance reasons.

✦ The asset's value supports safeguard selection decisions.

✦ The asset valuation might be necessary to satisfy due care and prevent negligence and legal liability.

Elements that Determine the Value of an Asset

Three basic elements determine an information asset's value:

1. The initial and ongoing cost (to an organization) of purchasing, licensing, developing, and supporting the information asset

2. The asset's value to the organization's production operations, research and development, and business model viability

3. The asset's value established in the external marketplace and the estimated value of the intellectual property (trade secrets, patents, copyrights, and so forth)

Safeguard Selection Criteria

Once the risk analysis has been completed, safeguards and countermeasures must be researched and recommended. There are several standard principles that are used in the selection of safeguards to ensure that a safeguard is properly matched to a threat and to ensure that a given safeguard most efficiently implements the necessary controls. Important criteria must be examined before selecting an effective countermeasure.

Cost-Benefit Analysis

The number one safeguard selection criteria is the cost effectiveness of the control to be implemented, which is derived through the process of the cost-benefit analysis. To determine the total cost of the safeguard, many elements need to be considered (including the following):

✦ The purchase, development, and/or licensing costs of the safeguard

✦ The physical installation costs and the disruption to normal production during the installation and testing of the safeguard

✦ Normal operating costs, resource allocation, and maintenance/repair costs

The simplest calculation to compute a cost-benefit for a given safeguard is as follows:

(ALE before safeguard implementation) – (ALE after safeguard implementation) – (annual safeguard cost) = value of safeguard to the organization

For example, if an ALE of a threat has been determined to be $10,000, the ALE after the safeguard implementation is $1,000, and the annual cost to operate the safeguard totals $500, then the value of a given safeguard is thought to be $8,500 annually. This amount is then compared against the startup costs, and the benefit or lack of benefit is determined.

This value can be derived for a single safeguard or can be derived for a collection of safeguards though a series of complex calculations. In addition to the financial cost-benefit ratio, other factors can influence the decision of whether to implement a specific security safeguard. For example, an organization is exposed to legal liability if the cost to implement a safeguard is less than the cost resulting from the threat realized and the organization does not implement the safeguard.

Level of Manual Operations

The amount of manual intervention required to operate the safeguard is also a factor in the choice of a safeguard. In case after case, vulnerabilities are created due to human error or an inconsistency in application. In contrast, automated systems require fail-safe defaults to allow for manual shutdown capability in case a vulnerability occurs. The more automated a process, the more sustainable and reliable that process will be.

In addition, a safeguard should not be too difficult to operate, and it should not unreasonably interfere with the normal operations of production. These characteristics are vital for the acceptance of the control by operating personnel and for acquiring the all-important management support required for the safeguard to succeed.

Auditability and Accountability Features

The safeguard must allow for the inclusion of auditing and accounting functions. The safeguard must also have the capability for auditors to audit and test it, and its accountability must be implemented to effectively track each individual who accesses the countermeasure or its features.

Recovery Ability

The safeguard's countermeasure should be evaluated with regard to its functioning state after activation or reset. During and after a reset condition, the safeguard must provide the following:

✦ No asset destruction during activation or reset

✦ No covert channel access to or through the control during reset

✦ No security loss or increase in exposure after activation or reset

✦ No operator access or rights in the default state until the controls are fully operational

Back Doors

A back door, maintenance hook, or trap door is a programming element that gives application maintenance programmers access to the internals of the application, thereby bypassing the normal security controls of the application. While this function is valuable for the support and maintenance of a program, the security practitioner must be aware of these doors and provide a means of control and accountability during their use.

Vendor Relations

The credibility, reliability, and past performance of the safeguard vendor must be examined. In addition, the openness (open source) of the application programming should also be known in order to avoid any design secrecy that prevents later modifications or allows unknown applications to have a back door into the system. Vendor support and documentation should also be considered.

Security Awareness

Although this section is our last for this chapter, it is not the least important. Security awareness is often an overlooked element of security management because most of a security practitioner's time is spent on controls, intrusion detection, risk assessment, and proactively or reactively administering security.

It should not be that way, however. People are often the weakest link in a security chain because they are not trained or generally aware of what security is all about. Employees must understand how their actions, even seemingly insignificant actions, can greatly impact the overall security position of an organization.

Employees must be aware of the need to secure information and to protect the information assets of an enterprise. Operators need training in the skills that are required to fulfill their job functions securely, and security practitioners need training to implement and maintain the necessary security controls.

All employees need education in the basic concepts of security and its benefits to an organization. The benefits of the three pillars of security awareness training — awareness, training, and education — will manifest themselves through an improvement in the behavior and attitudes of personnel and through a significant improvement in an enterprise's security.

The purpose of computer security awareness, training, and education is to enhance security by:

✦ Improving awareness of the need to protect system resources

✦ Developing skills and knowledge so computer users can perform their jobs more securely

✦ Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems

An effective computer security awareness and training program requires proper planning, implementation, maintenance, and periodic evaluation. In general, a computer security awareness and training program should encompass the following seven steps*:

1. Identify program scope, goals, and objectives.

2. Identify training staff.

3. Identify target audiences.

4. Motivate management and employees.

5. Administer the program.

6. Maintain the program.

7. Evaluate the program.

Making computer system users aware of their security responsibilities and teaching them correct practices helps users change their behavior. It also supports individual accountability because without the knowledge of the necessary security measures and to how to use them, users cannot be truly accountable for their actions.

Awareness

As opposed to training, security awareness refers to an organization's personnel being generally, collectively aware of the importance of security and security controls. In addition to the benefits and objectives we previously mentioned, security awareness programs also have the following benefits:

✦ Make a measurable reduction in the unauthorized actions attempted by personnel.

✦ Significantly increase the effectiveness of the protection controls.

✦ Help to avoid the fraud, waste, and abuse of computing resources.

---

*Source: NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems."

The Need for User Security Training

All personnel using a system should have some kind of security training that is specific either to the controls employed or to general security concepts. Training is especially important for those users who are handling sensitive or critical data. The advent of the microcomputer and distributed computing has created an opportunity for the serious failures of confidentiality, integrity, and availability.

Personnel are considered "security aware" when they clearly understand the need for security, how security impacts viability and the bottom line, and the daily risks to computing resources.

It is important to have periodic awareness sessions to orient new employees and refresh senior employees. The material should always be direct, simple, and clear. It should be fairly motivational and should not contain a lot of techno-jargon, and you should convey it in a style that the audience easily understands. The material should show how the security interests of the organization parallel the interest of the audience and how they are important to the security protections.

Let's list a few ways that security awareness can be improved within an organization without a lot expense or resource drain:

Live/interactive presentations. Lectures, videos, and computer-based training (CBT).

Publishing/distribution. Posters, company newsletters, bulletins, and the intranet.

Incentives. Awards and recognition for security-related achievement.

Reminders. Login banner messages and marketing paraphernalia such as mugs, pens, sticky notes, and mouse pads.

One caveat here: It is possible to oversell security awareness and to inundate personnel with a constant barrage of reminders. This will most likely have the effect of turning off their attention. It is important to find the right balance of selling security awareness. An awareness program should be creative and frequently altered to stay fresh.

Training and Education

Training is different from awareness in that it utilizes specific classroom or one-on-one training. The following types of training are related to InfoSec:

✦ Security-related job training for operators and specific users

✦ Awareness training for specific departments or personnel groups with security-sensitive positions

✦ Technical security training for IT support personnel and system administrators

✦ Advanced InfoSec training for security practitioners and information systems auditors

✦ Security training for senior managers, functional managers, and business unit managers

In-depth training and education for systems personnel, auditors, and security professionals is very important and is considered necessary for career development. In addition, specific product training for security software and hardware is vital to the protection of the enterprise.

A good starting point for defining a security training program could be the topics of policies, standards, guidelines, and procedures that are in use at an organization. A discussion of the possible environmental or natural hazards or a discussion of recent common security errors or incidents — without blaming anyone publicly — could work. Motivating the students is always the prime directive of any training, and their understanding of the value of security's impact to the bottom line is also vital. A common training technique is to create hypothetical security vulnerability scenarios and then to get the students' input on the possible solutions or outcomes.

✦   ✦   ✦

Assessment Questions

You can find the answers to the following questions in Appendix A.

1. Which choice below is an incorrect description of a control?

    a. Detective controls discover attacks and trigger preventative or corrective controls.

    b. Corrective controls reduce the likelihood of a deliberate attack.

    c. Corrective controls reduce the effect of an attack.

    d. Controls are the countermeasures for vulnerabilities.

2. Which statement below is accurate about the reasons to implement a layered security architecture?

    a. A layered security approach is not necessary when using COTS products.

    b. A good packet-filtering router will eliminate the need to implement a layered security architecture.

    c. A layered security approach is intended to increase the work-factor for an attacker.

    d. A layered approach doesn't really improve the security posture of the organization.

3. Which choice below represents an application or system demonstrating a need for a high level of confidentiality protection and controls?

    a. Unavailability of the system could result in inability to meet payroll obligations and could cause work stoppage and failure of user organizations to meet critical mission requirements. The system requires 24-hour access.

    b. The application contains proprietary business information and other financial information, which if disclosed to unauthorized sources, could cause an unfair advantage for vendors, contractors, or individuals and could result in financial loss or adverse legal action to user organizations.

    c. Destruction of the information would require significant expenditures of time and effort to replace. Although corrupted information would present an inconvenience to the staff, most information, and all vital information, is backed up by either paper documentation or on disk.

    d. The mission of this system is to produce local weather forecast information that is made available to the news media forecasters and the general public at all times. None of the information requires protection against disclosure.

4. Which choice below is NOT a concern of policy development at the high level?

   a. Identifying the key business resources

   b. Identifying the type of firewalls to be used for perimeter security

   c. Defining roles in the organization

   d. Determining the capability and functionality of each role

5. Which choice below is NOT an accurate statement about the visibility of IT security policy?

   a. The IT security policy should not be afforded high visibility.

   b. The IT security policy could be visible through panel discussions with guest speakers.

   c. The IT security policy should be afforded high visibility.

   d. The IT security policy should be included as a regular topic at staff meetings at all levels of the organization.

6. Which question below is NOT accurate regarding the process of risk assessment?

   a. The likelihood of a threat must be determined as an element of the risk assessment.

   b. The level of impact of a threat must be determined as an element of the risk assessment.

   c. Risk assessment is the first process in the risk management methodology

   d. Risk assessment is the final result of the risk management methodology.

7. Which choice below would NOT be considered an element of proper user account management?

   a. Users should never be rotated out of their current duties.

   b. The users' accounts should be reviewed periodically.

   c. A process for tracking access authorizations should be implemented.

   d. Periodically re-screen personnel in sensitive positions.

8. Which choice below is NOT one of NIST's 33 IT security principles?

   a. Implement least privilege.

   b. Assume that external systems are insecure.

   c. Totally eliminate any level of risk.

   d. Minimize the system elements to be trusted.

9. How often should an independent review of the security controls be performed, according to OMB Circular A-130?

    a. Every year

    b. Every three years

    c. Every five years

    d. Never

10. Which choice below BEST describes the difference between the System Owner and the Information Owner?

    a. There is a one-to-one relationship between system owners and information owners.

    b. One system could have multiple information owners.

    c. The Information Owner is responsible for defining the system's operating parameters.

    d. The System Owner is responsible for establishing the rules for appropriate use of the information.

11. Which choice below is NOT a generally accepted benefit of security awareness, training, and education?

    a. A security awareness program can help operators understand the value of the information.

    b. A security education program can help system administrators recognize unauthorized intrusion attempts.

    c. A security awareness and training program will help prevent natural disasters from occurring.

    d. A security awareness and training program can help an organization reduce the number and severity of errors and omissions.

12. Who has the final responsibility for the preservation of the organization's information?

    a. Technology providers

    b. Senior management

    c. Users

    d. Application owners

13. Which choice below is NOT an example of an issue-specific policy?

    a. Email privacy policy

    b. Virus-checking disk policy

    c. Defined router ACLs

    d. Unfriendly employee termination policy

14. Which statement below is NOT true about security awareness, training, and educational programs?

    a. Awareness and training help users become more accountable for their actions.

    b. Security education assists management in determining who should be promoted.

    c. Security improves the users' awareness of the need to protect information resources.

    d. Security education assists management in developing the in-house expertise to manage security programs.

15. Which choice below is an accurate statement about standards?

    a. Standards are the high-level statements made by senior management in support of information systems security.

    b. Standards are the first element created in an effective security policy program.

    c. Standards are used to describe how policies will be implemented within an organization.

    d. Standards are senior management's directives to create a computer security program.

16. Which choice below is a role of the Information Systems Security Officer?

    a. The ISO establishes the overall goals of the organization's computer security program.

    b. The ISO is responsible for day-to-day security administration.

    c. The ISO is responsible for examining systems to see whether they are meeting stated security requirements.

    d. The ISO is responsible for following security procedures and reporting security problems.

17. Which statement below is NOT correct about safeguard selection in the risk analysis process?

    a. Maintenance costs need to be included in determining the total cost of the safeguard.

    b. The best possible safeguard should always be implemented, regardless of cost.

    c. The most commonly considered criteria is the cost effectiveness of the safeguard.

    d. Many elements need to be considered in determining the total cost of the safeguard.

18. Which choice below is usually the number-one-used criterion to determine the classification of an information object?

    a. Value

    b. Useful life

    c. Age

    d. Personal association

19. What are high-level policies?

    a. They are recommendations for procedural controls.

    b. They are the instructions on how to perform a Quantitative Risk Analysis.

    c. They are statements that indicate a senior management's intention to support InfoSec.

    d. They are step-by-step procedures to implement a safeguard.

20. Which policy type is MOST likely to contain mandatory or compulsory standards?

    a. Guidelines

    b. Advisory

    c. Regulatory

    d. Informative

21. What does an Exposure Factor (EF) describe?

    a. A dollar figure that is assigned to a single event

    b. A number that represents the estimated frequency of the occurrence of an expected threat

    c. The percentage of loss that a realized threat event would have on a specific asset

    d. The annual expected financial loss to an organization from a threat

22. What is the MOST accurate definition of a safeguard?

    a. A guideline for policy recommendations

    b. A step-by-step instructional procedure

    c. A control designed to counteract a threat

    d. A control designed to counteract an asset

23. Which choice MOST accurately describes the differences between standards, guidelines, and procedures?

    a. Standards are recommended policies, whereas guidelines are mandatory policies.

    b. Procedures are step-by-step recommendations for complying with mandatory guidelines.

    c. Procedures are the general recommendations for compliance with mandatory guidelines.

    d. Procedures are step-by-step instructions for compliance with mandatory standards.

24. What are the detailed instructions on how to perform or implement a control called?

    a. Procedures

    b. Policies

    c. Guidelines

    d. Standards

25. How is an SLE derived?

    a. (Cost – benefit) $\times$ (% of Asset Value)

    b. AV $\times$ EF

    c. ARO $\times$ EF

    d. % of AV – implementation cost

26. What is a noncompulsory recommendation on how to achieve compliance with published standards called?

    a. Procedures

    b. Policies

    c. Guidelines

    d. Standards

27. Which group represents the MOST likely source of an asset loss through inappropriate computer use?

    a. Crackers

    b. Hackers

    c. Employees

    d. Saboteurs

28. Which choice MOST accurately describes the difference between the role of a data owner versus the role of a data custodian?

    a. The custodian implements the information classification scheme after the initial assignment by the owner.

    b. The data owner implements the information classification scheme after the initial assignment by the custodian.

    c. The custodian makes the initial information classification assignments, whereas the operations manager implements the scheme.

    d. The custodian implements the information classification scheme after the initial assignment by the operations manager.

29. What is an ARO?

    a. A dollar figure assigned to a single event

    b. The annual expected financial loss to an organization from a threat

    c. A number that represents the estimated frequency of an occurrence of an expected threat

    d. The percentage of loss that a realized threat event would have on a specific asset

30. Which formula accurately represents an Annualized Loss Expectancy (ALE) calculation?

    a. $SLE \times ARO$

    b. Asset Value (AV) $\times EF$

    c. $ARO \times EF - SLE$

    d. % of $ARO \times AV$