

CHAPTER**1**

Security Management Practices

In our first chapter we will enter the domain of Security Management. Throughout this book you will see that many Information Systems Security (InfoSec) domains have several elements and concepts that overlap. While all other security domains are clearly focused, this domain, for example, introduces concepts that are extensively touched upon in both the Operations Security (Chapter 6) and Physical Security (Chapter 10) domains. We will try to point out those occasions where the material is repetitive, but be aware that if a concept is described in several domains, you will need to understand it.

From the published (ISC)² goals for the Certified Information Systems Security Professional candidate:

“The candidate will be expected to understand the planning, organization, and roles 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 polices; security awareness 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; employment agreements; employee hiring and termination practices; and the risk management practices and tools to identify, rate, and reduce the risk to specific resources.”

2 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

A professional will be expected to know the following:

- *Basic information about security management concepts*
- *The difference between policies, standards, guidelines, and procedures*
- *Security awareness concepts*
- *Risk management (RM) practices*
- *Basic information on classification levels*

Our Goals

We will examine the InfoSec domain of Security Management 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 (including Valuation Rationale)
- Security Awareness Training

Domain Definition

The InfoSec domain of Security Management incorporates the identification of the 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

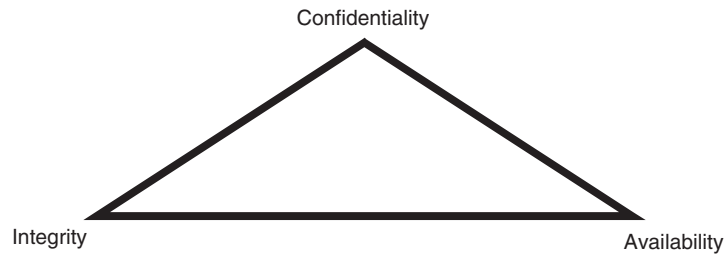


Figure 1.1 The C.I.A. triad.

- The objective of security controls—to reduce the impact of threats and the likelihood of their occurrence

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.

Confidentiality. In InfoSec, 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. In InfoSec, 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 are internally and externally consistent, i.e., that the internal information is consistent among all subentities and that the internal information is consistent with the real world, external situation.

Availability. In InfoSec, 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 they are needed. In addition, this concept guarantees that the security services needed by the security practitioner are in working order.

NOTE D.A.D. is the reverse of C.I.A.

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

4 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

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.

Identification. The means in 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 ability to determine the actions and behavior 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), which enable access to a computer resource. Once a user's identity and authentication are established, authorization levels determine the extent of system rights that an operator can hold.

Privacy. The level of confidentiality and privacy protection that a user is given 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.

Objectives of Security Controls

The prime objective of security controls is to reduce the effects of security threats and vulnerabilities to a level that is tolerable by an organization. This entails determining the impact a threat may have on an organization, and the likelihood that the threat could occur. The process that analyzes the threat scenario and produces a representative value of the estimated potential loss is called Risk Analysis (RA).

A small matrix can be created using an x - y graph where the y -axis represents the level of impact of a realized threat, and the x -axis represents the likelihood of the threat being realized, both set from low to high. When the matrix is created, it produces the graph shown in Figure 1.2. Remember the goal here is to reduce both the level of impact and the likelihood of a threat or disastrous event by implementing the security controls. A properly implemented control should move the plotted point from upper right—the threat value defined before the control was implemented—to the lower left (that is, toward 0,0), after the control was implemented. This concept is also very important when determining a control's cost/benefit ratio.

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 very badly designed controls, in the opposite direction) that it does not warrant the expense of implementation. In addition, the 0,0 point (no threat with no likelihood) is impossible

Threat vs. Likelihood Matrix

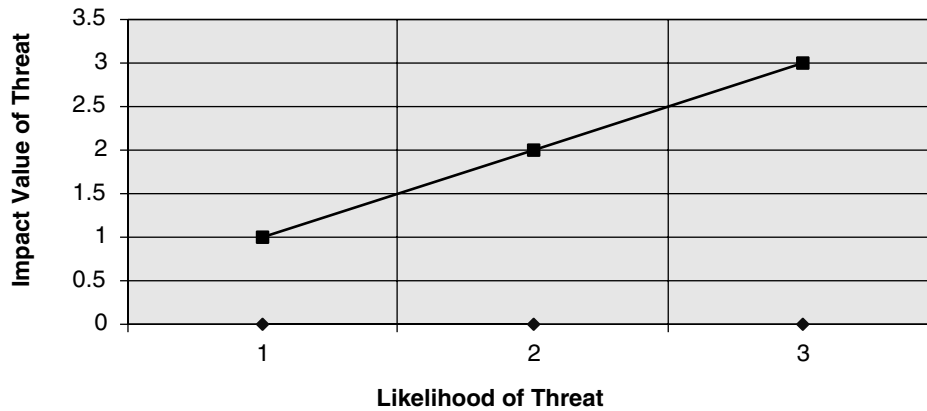


Figure 1.2 Threat versus likelihood matrix.

to achieve because a very unlikely threat could still have a measurement of .000001. Thus, it would still exist and possibly have a measurable impact. For example, the possibility that a flaming pizza delivery van will crash into the operations center is extremely unlikely, however, this potentially dangerous situation could still occur and have a fairly serious impact on the availability of computing resources.

A matrix with more greater than four subdivisions can be used for more detailed categorization of threats and impacts, if desired.

Information Classification Process

The first major InfoSec process we examine in this chapter is the concept of Information Classification. The Information Classification Process is related to the domains 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, and is 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

6 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

business unit or line operations 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, a more efficient cost-to-benefit ratio is achieved.

Information classification has the longest history in the government sector. Its value has been established, and it is a required component when securing trusted systems. In this sector, information classification is primarily used to prevent the unauthorized disclosure and the resultant failure of confidentiality.

Information classification may also be used to comply with privacy laws, or to enable regulatory compliance. A company may wish to employ classification to maintain a competitive edge in a tough marketplace. There may 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
- May be required for regulatory, compliance, or legal reasons

Information Classification Concepts

The information produced or processed by an organization 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 its 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 that is designated as neither sensitive nor classified. The public release of this information does not violate confidentiality.
2. *Sensitive but Unclassified (SBU)*. Information that has been designated as a minor secret, but may 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 that is 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 is used for documents labeled between SBU and Secret in sensitivity.
4. *Secret*. Information that is 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 (actually the President of the United States has a level only for him). 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 their 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. This information should probably not be disclosed. However, if it is disclosed, it is not expected to seriously or adversely impact the company.
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.
3. *Private*. Information that is considered of a personal nature and is intended for company use only. Its disclosure could adversely affect the company or its employees. For example, salary levels and medical information are considered private.
4. *Confidential*. Information that is considered very sensitive and is intended for internal use only. This information is exempt from disclosure under the Freedom of Information Act. Its unauthorized disclosure could seriously and negatively impact a company. For example, information about new product development, trade secrets, and merger negotiations is considered confidential.

Table 1.1 A Simple 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

8 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

Classification Criteria

Several criteria are 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 the information may 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 may need to be classified. For example, investigative information that reveals informant names may need to remain classified.

Information Classification Procedures

There are several steps in establishing a classification system. The following primary procedural steps are listed in priority order:

1. Identify the administrator/custodian.
2. Specify the criteria of how the information will be classified and labeled.
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 will be necessary are as follows:

- *Court order.* Classified information may need to be disclosed to comply with a court order.
- *Government contracts.* Government contractors may 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 may authorize the release of classified information to external entities or organizations. This release may 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 the users, owners, or custodians of the data play in regard to the data. The roles that owner, custodian, and user play in information classification are described and are important to remember.

Owner

An *information owner* may be an executive or manager of an organization. This person is responsible for the asset of information 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 may be liable for negligence because of the failure to protect this data. However, the actual day-to-day function of protecting the data belongs to a custodian.

The responsibilities of an information owner could include the following:

- Making the original determination to decide 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.

Custodian

An *information custodian* is delegated the responsibility of protecting the information by its owner. This role is commonly executed by IT systems personnel. The duties of a custodian may 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 *in accordance with* (IAW) the established information classification policy

In addition, the custodian may also have additional duties, such as being the administrator of the classification scheme.

10 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

User

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

- Users must follow the operating procedures that are 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.

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.

Security Policy Implementation

Security Policies are the basis for a sound security implementation. Often organizations will implement technical security solutions without first creating a foundation of policies, standards, guidelines, and procedures, which results in unfocused and ineffective security controls.

The following questions are discussed 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

Policies

A policy is one of those terms that can mean several things in InfoSec. 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 that is created on white paper, it is an essential and fundamental element of sound security practice. A policy, for example, can literally be a life saver during a disaster, or it may be a requirement of a governmental or regulatory function. A policy can also provide protection from liability due to an employee's actions, or can form a basis for the control of trade secrets.

Policy Types

When we refer to specific policies, rather than a group "policy," we are generally referring to those policies that are distinct from the standards, procedures, and guidelines. As you can see from the Policy Hierarchy chart shown 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, however, 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 tactical elements can follow.

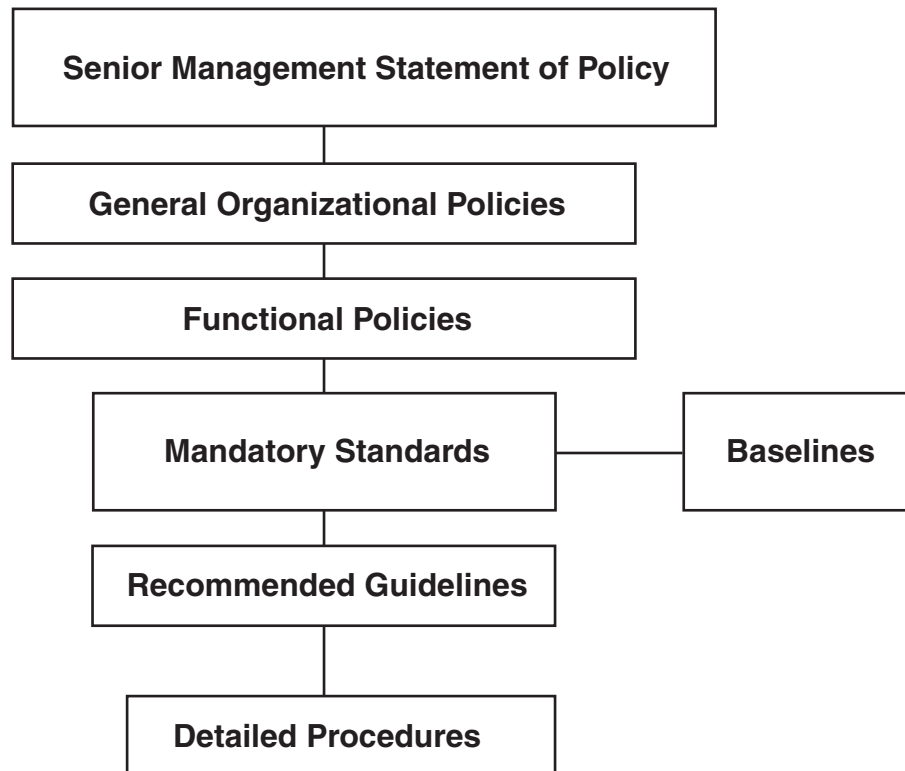


Figure 1.3 Policy hierarchy.

12 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

Senior Management Statement of Policy. The first policy of any policy creation 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

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 a 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.

Regulatory. *Regulatory policies* are security policies that an organization is required to implement, due to compliance, regulation, or other legal requirements. These companies may 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 organization operates.

Regulatory policies 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 they are following the standard and accepted industry policy.

Advisory. *Advisory policies* are security policies 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.

These policies can have many exclusions or application levels. Thus, some employees can be more controlled by these policies than others, according to their roles and responsibilities within that organization. For example, a policy that requires a certain procedure for transaction processing may 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.

However, penalties may be defined for the failure to follow a policy, such as the failure to follow a defined authorization procedure without stating what that policy is, and then referring the reader to another more detailed and confidential policy.

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 they 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 policies (especially the senior-level statement). Unfortunately, companies will often create one document that satisfies the needs of all of these elements; this is not good. There are a few good reasons why they should be kept separate:

- Each one 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 may need to be available to investors, but the procedures for changing passwords should not be available to anyone that 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 recommended actions only, and are not compulsory. Guidelines are more flexible than standards, and take into consideration the varying nature of the information systems. Guidelines may be used to specify the way standards should be developed, for example, or to guarantee the adherence to general security principles. The Rainbow series, described in Appendix B, and the Common Criteria, discussed in Appendix G, are considered guidelines.

14 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

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

Baselines. We mention *baselines* here because they are similar to standards, yet are a little different. Once a consistent set of baselines has been created, the security architecture of an organization can be designed, and standards can then be developed. Baselines take into consideration the difference between various operating systems, for example, to assure that the security is being uniformly implemented throughout the enterprise. If adopted by the organization, baselines are compulsory.

Roles and Responsibilities

The phrase “roles and responsibilities” pops up quite frequently in InfoSec. InfoSec controls are often defined by the job or role an employee plays in an organization. Each of these roles has data security rights and responsibilities. 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. It is important that individual roles and responsibilities are clearly communicated and understood (see Table 1.2).

All of the following concepts are fully defined in Chapter 6, “Operations Security,” but we discuss them briefly here:

Senior Management. Executive or senior-level management is assigned the overall responsibility for the security of information. Senior management may 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. 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. Previously discussed in the section titled “Information Classification Roles,” users are responsible for following the procedures, which are 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

Table 1.2 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 C.I.A.
User/Operator	Performs IAW the stated policies.
Auditor	Examines security.

the security policies, standards, guidelines, and procedures are effectively complying with the company's stated security objectives.

Risk Management

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

The identification of risk to an organization entails defining the four 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 formula and processes are designed to help provide some certainty when answering these questions. It should be pointed out, however, that because life and nature are constantly evolving and changing, not every possibility can be considered. Risk Management tries as much as possible to see the future and to lower the possibility of threats impacting a company.

NOTE Mitigating Risk

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

16 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

Principles of Risk Management

The Risk Management 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, some properties of the various elements will need to be determined, 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 likely, that threat will occur. To do this, 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 a Risk Analysis—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 a Risk Analysis. 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 also helps a company to 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 affect C.I.A., confidentiality, integrity, availability, overall or it could have a discrete dollar value—it could be tangible or intangible. It could also affect the full 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 occurrence of any 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 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 threat, or a 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 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. It is derived from the following formula:

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

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 primarily defined 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 in which a threat is expected to occur. The range for this value can be from 0.0 (never) to a large number (for minor threats, 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 number of employees that could make that error occur. The loss incurred by this event is not a concern here, only how often it does occur.

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. Whereas 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:

18 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

Table 1.3 Risk Analysis Formulas

CONCEPT	DERIVATION FORMULA
Exposure Factor (EF)	% of asset loss caused by threat.
Single Loss Expectancy (SLE)	Asset Value \times Exposure Factor (EF).
Annualized Rate of Occurrence (ARO)	Frequency of threat occurrence per year.
Annualized Loss Expectancy (ALE)	Single Loss Expectancy (SLE) \times Annualized Rate of Occurrence (ARO).

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 helps to provide a more reliable cost versus benefit analysis. Remember that the SLE is derived from the asset value and the Exposure Factor (EF). Table 1.3 shows these formulas.

Overview of Risk Analysis

We will 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 the other issues, rather than 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. However, fully quantitative risk analysis is not possible because qualitative measures must be applied. Thus, the reader 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, a detailed process plan must also be created, and roles must be assigned to the RA team.

Preliminary Security Examination (PSE). A PSE is often conducted before the actual quantitative RA. The PSE helps to gather the elements that will be needed 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.

AUTOMATED RISK ANALYSIS PRODUCTS

There are several good automated risk analysis products on the market. The main objectives of these products is to minimize the manual effort that must be expended to create the risk analysis and to provide a company with the ability to forecast its expected losses quickly with different input variations. The creation of a database during an initial automated process enables the operator to rerun the analysis 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.

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 6, "Operations Security"). However, a risk analysis is commonly much more comprehensive 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 (this is described in more detail later). This 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.

20 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

All types of threats should be considered in this section, no matter if they seem likely or not. It may 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, the misuse of technology by authorized users, tampering by disgruntled employees, or falsified data input

Application/Operational. 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 the SLE and ARO have been determined, we can estimate the ALE using the formula 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 its possible occurrence rate
- Loss potential by a threat—the dollar impact the threat will have on an asset
- Recommended remedial measures and safeguards or countermeasures

Remedies

There are three generic remedies to risk, which may 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 is 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 potential loss to which assets, and selects the 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 1.4 for a simple exposure rating scale.

Table 1.4 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

22 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

The procedures in performing the scenario are as follows:

- A scenario is written that addresses each major threat.
- The scenario is reviewed by business unit managers for a reality check.
- The RA team recommends and evaluates the various safeguards for each threat.
- The RA team works through each finalized scenario 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 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 often results in a control that either is ill-suited for asset protection, not financially effective, or it protects the wrong asset. Table 1.5 discusses quantitative versus qualitative RA.

Reasons for Determining the Value of an Asset

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

Table 1.5 Quantitative vs. 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

- The asset valuation is necessary to perform the cost/benefit analysis.
- The asset's value may be necessary for insurance reasons.
- The asset's value supports safeguard selection decisions.
- The asset valuation may be necessary to satisfy "due care" and prevent negligence and legal liability.

Elements that Determine the Value of an Asset

There are three basic elements that are used to determine an information asset's value:

1. The initial and on-going 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 safeguard most efficiently implements the necessary controls. Important criterion must be examined before selecting an effective countermeasure.

Cost/Benefit Analysis

The number one safeguard selection criteria is the cost effectiveness of the control that is to be implemented, which is derived through the process of the cost versus benefit analysis. To determine the total cost of the safeguard, many elements need to be considered, which include 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:

$$(\text{ALE before safeguard implementation}) - (\text{ALE after safeguard implementation}) - (\text{annual safeguard cost}) = \text{value of safeguard to the organization}$$

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 may be derived for a single safeguard, or can be derived for a collection of safeguards through a series of complex calculations. In addition to the financial

24 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

cost-to-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 fact, automated systems require fail-safe defaults to allow for manual shutdown capability in case a vulnerability occurs. The more automated a process is, 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 that is 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 have the ability to be audited and tested by the auditors, 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 in 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
- Defaults to a state that does not enable any operator access or rights until the controls are fully operational

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 application to have back doors into the system. Vendor support and documentation should also be considered.

BACK DOORS

A back door, maintenance hook, or trap door is a programming element that enables application maintenance programmers access to the internals of the application, thereby bypassing the normal security controls of the application. While this is a valuable function 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.

Security Awareness

Although this is our last section 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.

However, it should not be that way. People are often the weakest link in a security chain, often 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.

Awareness

As opposed to training, security awareness refers to the general, collective awareness of an organization's personnel of the importance of security and security controls. In addition to the benefits and objectives we have 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

Personnel are considered to be "security aware" when they clearly understand the need for security, and 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 should be conveyed in a style easily understood by the audience. 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, and without a lot expense or resource drain.

- *Live/Interactive Presentations.* Lectures, video, and Computer Based Training (CBT)

26 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

- *Publishing/Distribution.* Posters, company newsletters, bulletins, and the intranet
- *Incentives.* Awards and recognition for security-related achievement
- *Reminders.* Login-banner messages, marketing paraphernalia such as mugs, pens, sticky notes, and mouse pads

One caveat here: It is possible to oversell security awareness and to inundate the 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 also 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 the 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 the security's impact to the bottom line is also vital. A common training technique is to create hypothetical security vulnerability scenarios and to get the students' input on the possible solutions or outcomes.

THE NEED FOR USER SECURITY TRAINING

All personnel using a system should have some kind of security training that is either specific to the controls employed or 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.

Sample Questions

Answers to the Sample Questions for this and the other chapters are found in Appendix C.

1. 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. $\% \text{ of } ARO \times AV$
2. What is an ARO?
 - a. A dollar figure that is 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 a realized threat event would have on a specific asset
3. Which choice MOST accurately describes the difference between the role of a data owner versus the role of 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 and the operations manager implements the scheme.
 - d. The custodian implements the information classification scheme after the initial assignment by the operations manager.
4. Which choice is NOT an accurate description of C.I.A.?
 - a. C stands for confidentiality
 - b. I stands for integrity
 - c. A stands for availability
 - d. A stands for authorization
5. Which group represents the MOST likely source of an asset loss through inappropriate computer use?
 - a. Crackers
 - b. Hackers
 - c. Employees
 - d. Saboteurs

28 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

6. Which choice is the BEST description of authentication, as opposed to authorization?
 - a. The means in which a user provides a claim of their identity to a system
 - b. The testing or reconciliation of evidence of a user's identity
 - c. A system's ability to determine the actions and behavior of a single individual within a system
 - d. The rights and permissions granted to an individual to access a computer resource
7. What is a noncompulsory recommendation on how to achieve compliance with published standards called?
 - a. Procedures
 - b. Policies
 - c. Guidelines
 - d. Standards
8. Place the following four information classification levels in their proper order, from the least sensitive classification to the most sensitive.
 - a. SBU
 - b. Top secret
 - c. Unclassified
 - d. Secret
9. How is an SLE derived?
 - a. $(\text{Cost} - \text{benefit}) \times (\% \text{ of Asset Value})$
 - b. $AV \times EF$
 - c. $ARO \times EF$
 - d. $\% \text{ of AV} - \text{implementation cost}$
10. What are the detailed instructions on how to perform or implement a control called?
 - a. Procedures
 - b. Policies
 - c. Guidelines
 - d. Standards
11. What is the BEST description of risk reduction?
 - a. Altering elements of the enterprise in response to a risk analysis
 - b. Removing all risk to the enterprise at any cost
 - c. Assigning any costs associated with risk to a third party
 - d. Assuming all costs associated with the risk internally

12. Which choice MOST accurately describes the differences between standards, guidelines, and procedures?
 - a. Standards are recommended policies and 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.
13. A purpose of a security awareness program is to improve
 - a. The security of vendor relations.
 - b. The performance of a company's intranet.
 - c. The possibility for career advancement of the IT staff.
 - d. The company's attitude about safeguarding data.
14. 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
15. 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 a realized threat event would have on a specific asset
 - d. The annual expected financial loss to an organization from a threat
16. Which choice would be an example of a cost-effective way to enhance security awareness in an organization?
 - a. Train every employee in advanced InfoSec
 - b. Create an award or recognition program for employees
 - c. Calculate the cost-to-benefit ratio of the asset valuations for a risk analysis
 - d. Train only managers in implementing InfoSec controls
17. What is the prime directive of Risk Management?
 - a. Reduce the risk to a tolerable level
 - b. Reduce all risk regardless of cost
 - c. Transfer any risk to external third parties
 - d. Prosecute any employees that are violating published security policies

30 The CISSP Prep Guide: Mastering the Ten Domains of Computer Security

18. Which choice MOST closely depicts the difference between qualitative and quantitative risk analysis?
 - a. A quantitative RA does not use the hard costs of losses and a qualitative RA does.
 - b. A quantitative RA uses less guesswork than a qualitative RA.
 - c. A qualitative RA uses many complex calculations.
 - d. A quantitative RA cannot be automated.
19. Which choice is NOT a good criteria for selecting a safeguard?
 - a. The ability to recover from a reset with the permissions set to “allow all”
 - b. Comparing the potential dollar loss of an asset to the cost of a safeguard
 - c. The ability to recover from a reset without damaging the asset
 - d. The accountability features for tracking and identifying operators
20. Which policy type is MOST likely to contain mandatory or compulsory standards?
 - a. Guidelines
 - b. Advisory
 - c. Regulatory
 - d. Informative
21. 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.