Security-Management Practices

Terms you’ll need to understand:
✓ Confidentiality
✓ Integrity
✓ Availability
✓ Threat
✓ Vulnerability
✓ Public/private data classification
✓ Government data classification
✓ Risk
✓ SLE
✓ Residual risk
✓ ALE

Techniques you’ll need to master:
✓ Risk management
✓ Qualitative analysis
✓ Quantitative analysis
✓ Data-classification criteria
✓ Security roles
✓ Risk calculations
Introduction

This chapter helps the reader prepare for the security-management domain. Security management addresses the identification of the organization’s information assets. The security-management domain also introduces some critical documents, such as policies, procedures, and guidelines. These documents are of great importance because they spell out how the organization manages its security practices and details what is most important to the organization.

These documents are not developed in a void. Senior management helps point out the general direction, and risk-assessment and risk-analysis activities are used to determine where protective mechanisms should be placed. This chapter also introduces the two ways to calculate risk: qualitatively and quantitatively.

Finally, it’s important to not forget the employees. Employees need to be trained on what good security is and what they can do to ensure that good security is always practiced in the workplace. The goal here, as in other domains, is to ensure confidentiality, integrity, and availability of the organization’s assets and information. This chapter divides security-management practices into five broad categories:

➤ Risk assessment
➤ Policy
➤ Implementation
➤ Training and education
➤ Auditing the security infrastructure

Before we jump into these topics and look at the ways in which informational assets are protected, let’s talk briefly about the risks of poor security management and the role of confidentiality, integrity, and availability.

The Risk of Poor Security Management

Without policies and security-management controls in place, the organization is really saying that anything goes. That opens the organization to a host of risks, both internal and external. Examples of internal threats include leakage
of sensitive data, theft, legal liability, and corruption of data. External threats include natural disasters, spyware, viruses, worms, and Trojan programs. This is by no means a complete list, but it should alert you to the many dangers that organizations face each day. Failure to deal with these threats can lead to loss of information assets, reduced profits, civil or criminal suits, or even the demise of the company.

The Role of CIA

The three fundamental items upon which security is based together are known as the CIA triad (see Figure 3.1). You will see these concepts presented throughout this book.

Figure 3.1  CIA security triad.

➤ Confidentiality—The concept of keeping private information away from individuals who should not have access. Any time there is an unintentional release of information, confidentiality is lost. As an example, if Black Hat Bob can intercept an email between the CEO and the CIO and learn their latest plans, confidentiality has been broken and there is a lapse of security. Other attacks on confidentiality include sniffing, keystroke monitoring, and shoulder surfing.

➤ Integrity—The concept of integrity means that data is consistent and that it hasn’t been modified. This modification can result from access by an authorized or unauthorized individual or process. Integrity must also prevent modification of data while in storage or in transit. For example, if I could access my bank account and change the bank balance by adding a few zeroes . . . well, that’s not such a big deal to me, but the bank might not be happy because they would suffer a serious lapse of integrity.
➤ Availability—The concept of availability is pretty straightforward. You should have reliable and timely access to the data and resources you are authorized to use. A good example of a loss of availability is a DoS attack. No, it doesn’t give the perpetrator access, but it does prevent legitimate users from using the resource.

Which one of these three is most important? Well, that depends. They are all important, but organizations are unique. Different elements of the CIA triad will take the lead in different companies. For example, your local bank might consider integrity the most important, but an organization that does data processing might see availability as the primary concern.

Risk Assessment

A risk assessment is the process of identifying and prioritizing risks to the business. The assessment is crucial. Without an assessment, it is impossible to design good security policies and procedures that will defend your company’s critical assets. Risk assessment requires individuals to take charge of the risk-management process. These can be either senior management or lower-level employees. If senior management is driving the process, it’s considered top-down security, which is the preferred method. After all, senior management knows the goals and objectives of the company and are ultimately responsible. With senior management’s support, security will gain added importance. Management can also set the tone and direction of the security program and can define what is most critical.

Bottom-up security refers to a process by which lower-ranking individuals or groups of individuals attempt to implement better security-management practices without the active support of senior management. Bottom-up security places these individuals in a situation that’s unlikely to be successful. Without support from senior management, employees typically don’t see risk management and good security practices as being that important. Even if these individuals can successfully determine risks and suggest good controls, they’ll have a hard time procuring the needed funds for implementation.

Risk Management

Risk management is the act of determining what threats your organization faces, analyzing your vulnerabilities to assess the threat level, and determining how you will deal with the risk. Some of the major parts of risk management
Security-Management Practices

include developing the risk-management team, identifying threats and vulnerabilities, placing a value on the organization's assets, and determining how you will deal with the risk you uncover. The following definitions are important to know for risk management:

➤ **Threat**—A natural or man-made event that could have some type of negative impact on the organization.

➤ **Vulnerability**—A flaw, loophole, oversight, or error that can be exploited to violate system security policy.

➤ **Controls**—Mechanisms used to restrain, regulate, or reduce vulnerabilities. Controls can be corrective, detective, preventive, or deterrent.

Before you spend too much time struggling with all these concepts, take a moment to review Figure 3.2, which displays the relationship among threats, vulnerabilities, and controls. Notice that a threat by itself does not represent a danger and is not sufficient for a successful attack. A threat agent is required for an attack to be successful. A threat agent can be described as any circumstance or event that has the potential to cause harm to information assets through destruction, disclosure, or modification. Figure 3.2 uses an example threat of someone hacking a web server. Although it's true that anyone can attempt to attack a web server, the attacker needs a threat agent to be successful. The threat agent is described in Figure 3.2 as unpatched web server software that the attacker can access.

![Figure 3.2 Threats, vulnerabilities, and controls.](image-url)
Risk-Management Team
Don’t start thinking that this is a job you are going to take on by yourself. Risk management is a big job. You’ll need co-workers and employees from other departments to help. To do an effective job of risk-management analysis, you must involve individuals from all the different departments of the company. Otherwise, you run the risk of not seeing the big picture. It would be hard for any one person to understand the inner workings of all departments.

Sure, as an IT or security administrator, you understand the logical risk the IT infrastructure faces, but do you really have a grasp of the problems HR might have? These might include employee controls, effective termination practices, and control of confidentiality information. Bringing in key employees from other functional areas is required if you expect the risk management process to be successful. Consider employees from the following groups:

- Information system security
- IT and operations management
- System and network administration
- Internal audit
- Physical security
- Business process and information owners
- Human resources
- Legal
- Physical safety

Identifying the Threats and Vulnerabilities
Identifying threats and vulnerabilities is another important part of the risk-management process. Earlier we discussed how a natural or man-made threat can have some type of negative impact on the organization. Now let’s look at where threats can come from. Threats can occur as a result of human or natural factors, and can be caused by internal or external events. Figure 3.3 details some common threats to security. This is not meant to be an all-inclusive list, but it should get you thinking about some of the ways in which the organization can be threatened. Threats can also occur because of many other reasons, such as errors in computer code, accidental buffer overflows, or the unintentional actions of employees.
Identifying threats, threat agents, and vulnerabilities is just one step of the process. Knowing the values of the assets that you are trying to protect is also important because it would be foolish to exceed the value of the asset by spending more on the countermeasure than the asset is worth. Organizations have only limited funds and resources, so countermeasures must be effectively deployed to guard what has been deemed most critical.

Without placing dollar values or using some other metric to assess these variables, how can you start to analyze the threats, vulnerabilities, and risks the organization faces? One approach is to develop a table such as the one shown in Table 3.1. This helps demonstrate the relationship among threats, vulnerabilities, and risk. For example, an intruder can represent a threat that exposes the organization to theft of equipment because there is no security guard or controlled entrance.

![Figure 3.3 Security threats.](image)

**Table 3.1 Threat, Vulnerability, and Risk**

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Threat</th>
<th>Exploit/Vulnerability</th>
<th>Exposed Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human factor internal threat</td>
<td>Intruder</td>
<td>No security guard or controlled entrance</td>
<td>Theft</td>
</tr>
<tr>
<td>Human factor external threat</td>
<td>Hacker</td>
<td>Misconfigured firewall</td>
<td>Stolen credit card information</td>
</tr>
<tr>
<td>Human factor internal threat</td>
<td>Current employee</td>
<td>Poor accountability; no audit policy</td>
<td>Loss of integrity; altered data</td>
</tr>
</tbody>
</table>

(continued)
Placing a Value on Assets
Now, before you can really manage risk, you must know what's most valuable to the organization. You need to put a value on the organization's assets. You might be thinking that by value, we are discussing dollar amounts. That is one way to assess value, called quantitative assessment. You also have the choice to perform a qualitative assessment. If you choose to perform a qualitative assessment, you won't be dealing with dollar amounts because this is usually scenario driven. Qualitative and quantitative assessment techniques are described more in the following two sections.

Quantitative Assessment
Quantitative assessment deals with numbers and dollar amounts. It attempts to assign a cost (monetary value) to the elements of risk assessment and to the assets and threats of a risk analysis.

To fully complete a quantitative risk assessment, all elements of the process (asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty, and probability) are quantified. Therein lies the problem with purely quantitative risk assessment: It is difficult, if not impossible, to assign dollar values to all elements; therefore, some qualitative measures must be applied to quantitative elements. A quantitative assessment requires substantial time and personnel resources. The quantitative assessment process involves the following three steps:

1. **Estimate potential losses (SLE)**—This step involves determining the single loss expectancy (SLE). SLE is calculated as follows:

   \[ \text{Single loss expectancy} = \text{Asset value} \times \text{Exposure factor} \]

   Items to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information,
and threats that might cause a delay in processing. The exposure factor is the measure or percent of damage that a realized threat would have on a specific asset.

2. **Conduct a threat analysis (ARO)**—The purpose of a threat analysis is to determine the likelihood of an unwanted event. The goal is to estimate the annual rate of occurrence (ARO). Simply stated, how many times is this expected to happen in one year?

3. **Determine annual loss expectancy (ALE)**—This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE). ALE is calculated as follows:

\[
\text{Annualized loss expectancy (ALE)} = \frac{\text{Single loss expectancy (SLE)}}{\text{Annualized rate of occurrence (ARO)}}
\]

When performing the calculations discussed in this section, you should include all associated costs, such as these:

- Lost productivity
- Cost of repair
- Value of the damaged equipment or lost data
- Cost to replace the equipment or reload the data

When these costs are accumulated and specific threats are determined, the annualized loss expectancy can be calculated. This builds a complete picture of the organization’s risk and allows the organization to plan an effective strategy.

Review Table 3.2; we can work through the virus risk example given there. First, you need to calculate the SLE. The SLE requires that you multiply the exposure factor by the asset value:

\[9,450 \times .17 = 1,650\]

The asset value is the value you have determined the asset to be worth. The exposure factor is the amount of damage that the risk poses to the asset. For example, the risk-management team might consult with its experts and determine that 17% of its Word documents and data could be destroyed from a virus.

Next, the ARO is calculated. The ARO is the frequency at which this event is expected to happen within a given period of time. For example, the experts might have determined that there is a 90% chance of this event occurring within a 1-year period.
Finally, the ALE is calculated. The ALE is the SLE multiplied by the ARO:

\[ \text{ALE} = \text{SLE} \times \text{ARO} \]

\[ \$1,650 \times .9 = \$1,485 \]

This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. You can interpret this figure to mean that the business should expect to lose an average of $1,485 each year due to computer viruses.

### Table 3.2 How SLE, ARO, and ALE Are Used

<table>
<thead>
<tr>
<th>Asset</th>
<th>Risk</th>
<th>Asset Value</th>
<th>Exposure Factor</th>
<th>SLE</th>
<th>Annualized Frequency</th>
<th>ALE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer database</td>
<td>Hacked</td>
<td>$432,000</td>
<td>.74</td>
<td>$320,000</td>
<td>.25</td>
<td>$80,000</td>
</tr>
<tr>
<td>Word documents and data files</td>
<td>Virus</td>
<td>$9,450</td>
<td>.17</td>
<td>$1,650</td>
<td>.9</td>
<td>$1,485</td>
</tr>
<tr>
<td>Domain controller failure</td>
<td>Server failure</td>
<td>$82,500</td>
<td>.88</td>
<td>$72,500</td>
<td>.25</td>
<td>$18,125</td>
</tr>
<tr>
<td>E-commerce website DDoS</td>
<td>DDoS</td>
<td>$250,000</td>
<td>.44</td>
<td>$110,000</td>
<td>.45</td>
<td>$49,500</td>
</tr>
</tbody>
</table>

Automated tools are available that minimize the effort of the manual process. These programs enable users to rerun the analysis with different parameters to answer “what-ifs.” They perform calculations quickly and can be used to estimate future expected losses easier than performing the calculations manually.

**ALERT**

A lot of math can be involved in a quantitative assessment, but the CISSP exam focuses on the SLE, ALE, and ARO formulas.

### Qualitative Assessment

Maybe you are thinking that there has to be another way to perform an assessment. If so, you are right. **Qualitative assessment** is scenario driven and does not attempt to assign dollar values to components of the risk analysis. Purely quantitative risk assessment is hard to achieve because some items are difficult to tie to fixed dollar amounts. Absolute qualitative risk analysis is possible because it ranks the seriousness of threats and sensitivity of assets into grades or classes, such as low, medium, and high. An example of this can be seen in NIST 800-26, a document that uses confidentiality, integrity, and
availability as categories of loss and then ranks each loss based on a scale of low, medium, and high. The ranking is subjective:

- **Low**—Minor inconvenience that could be tolerated for a short period of time.
- **Medium**—Could result in damage to the organization or cost a moderate amount of money to repair.
- **High**—Would result in loss of goodwill between the company and clients or employees. Could result in a legal action or fine, or cause the company to lose revenue or earnings.

Table 3.3 displays an example of how this process is performed. As you can see, no dollar amounts are used. Potential loss is only ranked as high, medium, or low.

<table>
<thead>
<tr>
<th>Asset</th>
<th>Loss of Confidentiality</th>
<th>Loss of Integrity</th>
<th>Loss of Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer database</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Internal documents</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Advertising literature</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>HR records</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
</tbody>
</table>

The downside of performing a qualitative assessment is that you are not working with dollar values, so it is sometimes harder to communicate the results of the assessment to management. Another downside is that it is derived from gut feelings or opinions of experts in the company, not always an “exact assessment” that senior management will want to receive from you.

Other types of qualitative assessment techniques include these:

- **The Delphi Technique**—A group assessment process that allows individuals to contribute anonymous opinions.
- **Facilitated Risk Assessment Process (FRAP)**—A subjective process that obtains results by asking questions. It is designed to be completed in a matter of hours, making it a quick process to perform.

### The NSA Information Assurance Methodology (IAM)

The NSA developed the IAM in 1998 in response to Presidential Decision Directive (PDD)-63. PDD-63 mandated that all federal computer systems be assessed to determine their overall security. The purpose of the IAM is to review an organization’s INFOSEC posture, identify potential vulnerabilities, and provide recommendations on their elimination or mitigation. It uses the security triad (confidentiality, integrity, and availability) as a basis of assessment.
Handling Risk

Now that you have been introduced to some of the ways to determine risk, you are tasked with making a decision on how to deal with what you have found. Risk can be dealt with in four general ways, either individually or in combination.

➤ **Risk reduction**—Implement a countermeasure to alter or reduce the risk.

➤ **Risk transference**—Purchase insurance to transfer a portion or all of the potential cost of a loss to a third party.

➤ **Risk acceptance**—Deal with risk by accepting the potential cost and loss if the risk occurs.

➤ **Risk rejection**—Pretend that the risk doesn’t exist and ignore it. Although this is not a prudent course of action, it is one that some organizations choose to take.

Which is the best way to handle risk? This depends on the cost of the countermeasure, the value of the asset, and the amount by which risk-reduction techniques reduce the total risk. Companies usually choose the one that provides the greatest risk reduction while maintaining the lowest annual cost. These concepts are expressed numerically as the following formulas:

\[
\text{Total risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset value}
\]

\[
\text{Residual risk} = \text{Total risk} - \text{Countermeasures}
\]

No organization can ever be 100% secure. There will always be remaining risk. The residual risk is the amount that is left after safeguards and controls have been put in place.

**NOTE**
What's cost-effective? The cost-effectiveness of a safeguard can be measured as follows:

\[
\text{ALE before the safeguard} - \text{ALE after the safeguard} = \text{Value of the safeguard to the organization}
\]

This formula can be used to evaluate the cost-effectiveness of a safeguard or to compare various safeguards to determine which are most effective. The higher the resulting value is, the more cost-effective the safeguard is.

Policies, Procedures, Standards, Baselines, and Guidelines

Security is truly a multilayered process. After an assessment is completed, policies will fall quickly in place because it will be much easier for the organization to determine security policies based on what has been deemed most
important from the risk assessments. The assessment should help drive policy creation on items such as these:

➤ Passwords
➤ Patch management
➤ Employee hiring and termination practices

Low-level checks are for employees starting at low-level jobs. Before they move to a higher-level position, additional checks should be performed.

➤ Backup practices and storage requirements
➤ Security awareness training
➤ Antivirus
➤ System setup and configuration

For security to be effective, it must start at the top of an organization. It must permeate every level of the hierarchy. Senior management must make decisions on what should be protected, how it should be protected, and to what extent it should be protected. These findings should be crafted into written documents.

Before these documents are locked in as policies, they must be researched to verify that they will be compliant with all federal, state, and local laws. These documents should also clearly state what is expected from employees and what the result of noncompliance will be.

**Security Policy**

Policies are the top tier of formalized security documents. These high-level documents offer a general statement about the organization’s assets and what level of protection they should have. Well-written policies should spell out who’s responsible for security, what needs to be protected, and what is an acceptable level of risk. They are much like a strategic plan because they outline what should be done but don’t specifically dictate how to accomplish the stated goals. Those decisions are left for standards, baselines, and procedures. Security policies can be written to meet advisory, informative, and regulatory needs. Each has a unique role or function.

The key element in policy is that it should state management’s intention toward security.
Advisory Policy
The job of an advisory policy is to ensure that all employees know the consequences of certain behavior and actions. Here’s an example advisory policy:

Illegal copying: Employees should never download or install any commercial software, shareware, or freeware onto any network drives or disks unless they have written permission from the network administrator. Be prepared to be held accountable for your actions, including the loss of network privileges, written reprimand, probation, or employment termination if the Rules of Appropriate Use are violated.

Informative Policy
This type of policy isn’t designed with enforcement in mind; it is developed for education. Its goal is to inform and enlighten employees. The following is an example informative policy:

In partnership with Human Resources, the employee ombudsman’s job is to serve as an advocate for all employees, providing mediation between employees and management. This job is to help investigate complaints and mediate fair settlements when a third party is requested.

Good policy strikes a balance and is both relevant and understandable. If a policy is too generic, no one will care what it says because it doesn’t apply to the company. If a policy is too complex, no one will read it—or understand it if they did.

Regulatory Policy
These policies are used to make certain that the organization complies with local, state, and federal laws. An example regulatory policy might state:

Because of recent changes to Texas State law, The Company will now retain records of employee inventions and patents for 10 years; all email messages and any backup of such email associated with patents and inventions will be stored for one year.

Standards
Standards are much more specific than policies. Standards are tactical documents because they lay out specific steps or processes required to meet a certain requirement. As an example, a standard might set a mandatory requirement that all email communication be encrypted. So although it does specify a certain standard, it doesn’t spell out how it is to be done. That is left for the procedure.
Baselines

A baseline is a minimum level of security that a system, network, or device must adhere to. Baselines are usually mapped to industry standards. As an example, an organization might specify that all computer systems comply with a minimum Trusted Computer System Evaluation Criteria (TCSEC) C2 standard. TCSEC standards are discussed in detail in Chapter 5, “System Architecture and Models.”

Guidelines

A guideline points to a statement in a policy or procedure by which to determine a course of action. It’s a recommendation or suggestion of how things should be done. It is meant to be flexible so it can be customized for individual situations.

Don’t confuse guidelines with best practices. Whereas guidelines are used to determine a recommended course of action, best practices are used to gauge liability. Best practices state what other competent security professionals would have done in the same or similar situation.

Procedures

A procedure is the most specific of security documents. A procedure is a detailed, in-depth, step-by-step document that details exactly what is to be done. As an analogy, when my mom sent my wife the secret recipe for a three-layer cake, it described step by step what needed to be done and how. It even specified a convection oven, which my mom stated was an absolute requirement.

Procedures are detailed documents, they are tied to specific technologies and devices (see Figure 3.4). You should expect to see procedures change as equipment changes. As an example, imagine that your company has replaced its CheckPoint firewall with a Cisco PIX. Although the policies and standards dictating the firewalls role in your organization probably will not change, the procedure for configuration of the firewall will.

It’s unfortunate that sometimes instead of the donkey leading the cart, the cart leads the donkey. By this, I mean that sometimes policies and procedures are developed as a result of a negative event or an audit. The audit or policy shouldn’t be driving the process; the assessment should be. The assessment’s purpose is to give management the tools needed to examine all currently identified concerns. From this, management can prioritize the level of exposure they are comfortable with and select an appropriate level of control. This level of control should then be locked into policy.
Implementation

You cannot implement what senior management won't support. Sure, you will need the employees to buy into the process, but the biggest element of success depends on making sure that security flows from the top. With senior management leading the way, you can further ensure success by setting up a data-classification scheme so that employees realize the importance of the data they work with. You will also want to consider employee training—without it, how will employees know good security practices? As a final step, you will want to build in security controls because they allow you to monitor the level of compliance.

Data Classification

Organizational information that is proprietary or confidential in nature must be protected. Data classification is a useful way to rank an organization’s informational assets. The two most common data-classification schemes are military and public. Companies store and process so much electronic information about their customers and employees that it’s critical for them to take appropriate precautions to protect this information. Both military and private data-classification systems accomplish this task by placing information into categories. The first step of this process is to assess the value of the information. When the value is known, it becomes much easier to decide what amount of resources should be used to protect the data. It would make no sense to spend more on protecting something with a lesser value or worth.

Each level of classification that is established should have specific requirements and procedures. The military and commercial data-classification models have predefined labels and levels. When an organization decides which model to use, it can evaluate data placement by using criteria such as the following:

➤ The value of the data
➤ Its age
Security-Management Practices

➤ Laws
➤ Regulations pertaining to its disclosure
➤ Replacement cost

Military Data Classification
The military data-classification system is widely used within the Department of Defense. This system has five levels of classification:

➤ Unclassified
➤ Sensitive
➤ Confidential
➤ Secret
➤ Top secret

Each level represents an increasing level of sensitivity. Sensitivity is the desired degree of secrecy that the information should maintain. If an individual holds a confidential clearance, it would mean that he could access unclassified, sensitive, or confidential information for which he has a need to know. His need-to-know would not extend to the secret or top secret levels. The concept of need-to-know is similar to the principle of least privilege, in that employees should have access only to information that they need to know to complete their assigned duties. Table 3.4 provides details about the military and public/private data-classification models.

Public/Private Data Classification
The public or commercial data classification is also built upon a four-level model:

➤ Public—This information might not need to be disclosed, but if it is, it shouldn’t cause any damage.

➤ Sensitive—This information requires a greater level of protection to prevent loss of confidentiality.

➤ Private—This information is for company use only, and its disclosure would damage the company.

➤ Confidential—This is the highest level of sensitivity, and disclosure could cause extreme damage to the company.
Table 3.4 Commercial and Military Data Classifications

<table>
<thead>
<tr>
<th>Commercial Business Classifications</th>
<th>Military Classifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Top secret</strong></td>
<td><strong>Top secret</strong></td>
</tr>
<tr>
<td><strong>Confidential</strong></td>
<td><strong>Secret</strong></td>
</tr>
<tr>
<td><strong>Private</strong></td>
<td><strong>Confidential</strong></td>
</tr>
<tr>
<td><strong>Sensitive</strong></td>
<td><strong>Sensitive</strong></td>
</tr>
<tr>
<td><strong>Public</strong></td>
<td><strong>Unclassified</strong></td>
</tr>
</tbody>
</table>

Information has a useful life. Data-classification systems need to build in mechanisms to monitor whether information has become obsolete. If that is the case, it should be declassified or destroyed.

Roles and Responsibility

Just as we have discussed the importance of data classification, it's important to provide a clear division of roles and responsibility. This will be a tremendous help when dealing with any security issues. Everyone should be subject to this policy, including employees, consultants, and vendors. The following list highlights some general areas of responsibility different organizational roles should be held to regarding organizational security. Common roles include owner, data custodian, user, and security auditor:

➤ **Data owner**—Usually a member of senior management. After all, senior management is responsible for the asset and, if it is compromised, can be held responsible. The data owner can delegate some day-to-day duties but cannot delegate total responsibility; senior management is ultimately responsible.

➤ **Data custodian**—This is usually someone in the IT department. The data custodian does not decide what controls are needed, but he or she does implement controls on behalf of the data owner. Other responsibilities include the day-to-day management of the asset. Controlling access, adding and removing privileges for individual users, and ensuring that the proper controls have been implemented are all part of the data custodian's daily tasks.

➤ **User**—This is a role that most of us are familiar with because this is the end user in an organization. Users do have responsibilities: They must comply with the requirements laid out in policies and procedures. They must also practice due care.
➤ Security auditor—This is the person who examines an organization’s security procedures and mechanisms. How often this process is performed depends on the industry and its related regulations. As an example, the health care industry is governed by the Health Insurance Portability and Accountability Act (HIPAA) regulations and states that audits must be performed yearly. Regardless of the industry, senior management should document and approve the audit process.

Security Controls

The objective of security controls is to enforce the security mechanisms the organization has developed. Security controls can be administrative, technical, or physical. With effective controls in place, risks and vulnerabilities can be reduced to a tolerable level. Security controls are put in place to protect confidentiality, integrity, and availability.

Administrative

Administrative controls are composed of the policies, procedures, guidelines, and baselines an organization develops. Administrative controls also include the mechanisms put in place to enforce and control employee activity and access, such as the following:

➤ Applicant screening—A valuable control that should be used during the hiring process. Background checks, reference checks, verification of educational records, and NDAs should all be part of the screening process.

➤ Employee controls—Another useful mechanism that can add defense in depth to the organization’s administrative controls. Some common employee controls include detailed job descriptions with defined roles and responsibilities. These are procedures that mandate the rotation of duties, the addition of dual controls, and mandatory vacations.

➤ Termination procedures—A form of administrative control that should be in place to address the termination of employees. Termination procedures should include exit interviews, review of NDAs, suspension of network access, and checklists verifying that employees have returned all equipment they had in their care, such as remote-access tokens, keys, ID cards, cellphones, pagers, credit cards, laptops, and software.
Technical
Technical controls are the logical mechanisms used to control access, authenticate users, identify unusual activity, and restrict unauthorized access. Some of the devices used as technical controls include firewalls, IDS systems, and authentication devices such as biometrics. Technical controls can be hardware or software.

Physical
Physical controls are the controls that are most typically seen. Examples of physical controls include gates, guards, fences, locks, CCTV systems, turnstiles, and mantraps. Because these controls can be seen, it’s important to understand that people might attempt to find ways to bypass them. You’ve probably seen this at a card key–controlled entrance: One person opens the door, and two or three walk in.

Because some controls will be highly visible, others should be designed as more covert, to ensure defense in depth.

Training and Education
Right or wrong, employees believe that it is up to employers to provide training. Without proper training, employees are generally unaware of how their actions or activities can affect the security of the organization. One of the weakest links in security is the people who work for the company. Social-engineering attacks prey on the fact that users are uneducated in good security practices; therefore, the greatest defense against these types of attacks is training, education, and security awareness (see Figure 3.5).
Besides security awareness, you might find that your employees need more in-depth training in matters of organizational security. This might consist of in-house training programs that teach new employees needed security skills or the decision to send the security staff offsite for a CISSP education program. Regardless of which program your company decides it needs, you can use seven steps to help determine what type of security training to sponsor:

1. Establish organizational technology objectives.
2. Conduct a needs assessment.
3. Find a training program that meets these needs.
4. Select the training methods and mode.
5. Choose a means of evaluating.
6. Administer training.
7. Evaluate the training.

Types of training include the following:

- In-house training
- Web-based training
- Classroom training
- Vendor training
- On-the-job training
- Apprenticeship programs
- Degreed programs
- Continuing education programs

Training and education are not the same. Training programs are of short duration and usually teach individuals a specific skill. Education is broader based and longer term. Degree programs are examples of education.

## Security Awareness

Awareness programs can be effective in increasing employee understanding of security. Security awareness training must be developed differently for the various groups of employees that make up the organization. Not only will the training vary, but the topics and types of questions you’ll receive from the participants will also vary. Successful employee awareness programs tailor the
message to fit the audience. These are three of the primary groups that security awareness training should be targeted to

➤ **Senior management**—Don’t try presenting an in-depth technical analysis to this group. They want to know the costs, benefits, and ramifications if good security practices are not followed.

➤ **Data custodians**—This group requires a more structured presentation on how good security practices should be implemented, who is responsible, and what the individual and departmental cost is for noncompliance.

➤ **Users**—This must align with an employee’s daily tasks and map to the user’s specific job functions.

---

**Employee-awareness programs work best when they are run for short periods and changed frequently.**

---

**The goal of security awareness is to increase management’s ability to hold employees accountable for their actions and to modify employee behavior toward security.**

---

**Auditing Your Security Infrastructure**

After all the previous items discussed in this chapter have been performed, the organization’s security-management practices will need to be evaluated periodically. This comes in the form of an *audit process*. This is the only way you can verify that the controls put in place are working, that the policies that were written are being followed, and that the training provided to the employees actually works. The audit process can also be used to verify that each individual’s responsibility is clearly defined. Employees should know their amount of accountability and what is considered their assigned duties.

---

**Without sound policies in place, it is not worth doing an audit because there is no adequate baseline on which to base the audit.**
Exam Prep Questions

1. Which of the following levels represent the military classification system?
   - A. Confidential, private, sensitive, and public
   - B. Top secret, secret, private, sensitive, and public
   - C. Top secret, confidential, private, sensitive, and unclassified
   - D. Top secret, secret, confidential, sensitive, and unclassified

2. This method of handling risk works by using a third party to absorb a portion of the risk.
   - A. Risk reduction
   - B. Risk transference
   - C. Risk acceptance
   - D. Risk rejection

3. You have been asked to calculate the annualized loss expectancy (ALE) for the following variables:
   - Single loss expectancy = $25
   - Exposure factor = .9
   - Annualized rate of occurrence = .4
   - Residual risk = $30
   A. $9.00
   B. $22.50
   C. $10.00
   D. $14.27

4. Place the following formulas in order:
   - A. ALE, residual risk, SLE, ARO
   - B. ALE, ARO, SLE, residual risk
   - C. ARO, SLE, ALE, residual risk
   - D. SLE, ARO, ALE, residual risk

5. The downside of performing this type of assessment is that you are not working with dollar values, so it is sometimes harder to communicate the results of the assessment to management.
   - A. Qualitative
   - B. Quantitative
   - C. Numeric mitigation
   - D. Red team

6. This category of control can include the logical mechanisms used to control access and authenticate users.
   - A. Administrative
   - B. Clerical
   - C. Technical
   - D. Physical
7. Which of the following formulas represents total risk?
   - A. Risk × Vulnerability × Asset value = Total risk
   - B. Threat × Vulnerability × Asset value = Total risk
   - C. Risk × Value/Countermeasure = Total risk
   - D. Threat − Vulnerability/Asset value = Total risk

8. Which of the following is a flaw, loophole, oversight, or error that makes an organization susceptible to attack or damage?
   - A. Risk
   - B. Vulnerability
   - C. Threat
   - D. Exploit

9. This is the most specific of security documents.
   - A. Procedures
   - B. Standards
   - C. Policies
   - D. Baselines

10. The last thing you want in an organization is that everyone is accountable but no one is responsible. Therefore, the data owner should be which of the following groups?
    - A. End users.
    - B. Technical managers.
    - C. Senior management.
    - D. Everyone is responsible; therefore, all groups are owners.
Answers to Exam Prep Questions

1. Answer: D. The military data-classification system is widely used within the Department of Defense. This system has five levels of classification: unclassified, sensitive, confidential, secret, and top secret. Each level represents an increasing level of sensitivity.

2. Answer: B. The purchase of insurance to transfer a portion or all of the potential cost of a loss to third party is known as risk transference. All other answers are incorrect: Risk reduction implements a countermeasure, risk acceptance deals with it by accepting the potential cost, and risk rejection pretends it doesn’t exist.

3. Answer: C. $25 \times .4 = $10$, or Single loss expectancy (SLE) $\times$ Annualized rate of occurrence (ARO) $=$ Annualized loss expectancy (ALE).

4. Answer: D. The quantitative assessment process involves the following steps: Estimate potential losses (SLE), conduct a threat analysis (ARO), determine annual loss expectancy (ALE), and determine the residual risk after a countermeasure has been applied.

5. Answer: A. Qualitative assessment is scenario driven and does not attempt to assign dollar values to components of the risk analysis. Quantitative assessment is based on dollar amounts; both numeric mitigation and red team are distracters.

6. Answer: C. Technical controls can be hardware or software. They are the logical mechanisms used to control access and authenticate users, identify unusual activity, and restrict unauthorized access. Clerical is a nonexistent category, and all other answers are incorrect: Administrative controls are procedural, and physical controls include locks, guards, gates, and alarms.

7. Answer: B. Risk is expressed numerically as follows:

   \[
   \text{Threat} \times \text{Vulnerability} \times \text{Asset value} = \text{Total risk}
   \]

   All other answers do not properly define the formula for total risk.

8. Answer: B. Vulnerability is a flaw, loophole, oversight, or error that makes the organization susceptible to attack or damage. All other answers are incorrect: A risk can be defined as the potential harm that can arise from some present process or from some future event; a threat is an unwanted event that can result in harm to an asset or service; and an exploit takes advantage of a bug, glitch, or vulnerability.

9. Answer: A. A procedure is a detailed, in-depth, step-by-step document that lays out exactly what is to be done. It’s a detailed document that is tied to specific technologies and devices. Standards are tactical documents; policies are high-level documents; and baselines are minimum levels of security that a system, network, or device must adhere to.
10. Answer: C. Senior management should be the ultimate owner because these individuals are responsible for the asset and must answer if a compromise occurs. Although answer C is the best possible choice, it is important to realize that, in most cases, the data owner will be a member of management but might not be the most senior position within the company. For example, the CFO would be the data owner for all financial data, the director of human resources would be the data owner for all HR data, and so on. All other answers are incorrect because end users, technical managers, and other employees are not typically the data owners.
Need to Know More?

www.jebcl.com/riskdo/riskdo.htm—Risk assessment do’s and don’ts

www.usatoday.com/money/jobcenter/workplace/recruiting/2002-11-20-legal_x.htm—Keeping pre-employment checks legal

http://library.lp.findlaw.com/articles/file/00334/002357/title/Subject/topic/Employment%20Law_At-will%20Employment/filename/employment_law_1_454—Self-audits of employment practices


http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci1033304,00.html—Ten traits of effective policy

www.sans.org/resources/policies/—Policy templates and information

www.itl.nist.gov/lab/bulletns/bltnoct03.htm—Building an effective security-awareness program

www.computerworld.com/careertopics/careers/training/story/0,10801,54375,00.html—Methods to build effective security awareness

www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/srgsch02.mspx—Risk-management guide