Chapter 1

Measuring and Weighing Risk

THE FOLLOWING COMPTIA SECURITY+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ 1.3 Distinguish and differentiate network design elements and compounds.
   ▪ Cloud computing: Platform as a Service; Software as a Service; Infrastructure as a Service

✓ 2.1 Explain risk related concepts.
   ▪ Control types: Technical; Management; Operational
   ▪ False positives
   ▪ Importance of policies in reducing risk: Privacy policy; Acceptable use; Security policy; Mandatory vacations; Job rotation; Separation of duties; Least privilege
   ▪ Risk calculation; Likelihood; ALE; Impact
   ▪ Quantitative vs. Qualitative
   ▪ Risk avoidance, transference, acceptance, mitigation, deterrence
   ▪ Risk associated to Cloud Computing and Virtualization

✓ 2.2 Carry out appropriate risk mitigation strategies.
   ▪ Implement security controls based on risk
   ▪ Change management
   ▪ Incident management
   ▪ User rights and permission reviews
   ▪ Perform routine audits

✓ 3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities.
   ▪ Risk calculations: Threat vs. likelihood

✓ 4.3 Explain the importance of data security.
   ▪ Cloud computing
As an administrator, you know that there are risks involved in working with data. You know that data can become corrupt, can be accessed by those who shouldn’t see it, can have values changed, and so on. If you think that being armed with this knowledge is enough to enable you to take the steps to keep any harm from happening, however, you’ll be sadly mistaken. One of the possible actions administrators can take to potential threats is to simply accept that they will happen. If the cost of preventing a particular risk from becoming a reality exceeds the value of the harm that could be caused by the event, then a cost/benefit risk calculation dictates that the risk should remain.

Most risk calculations weigh a potential threat against the likelihood of it occurring. As frustrating as it may seem, you should always be able to accept the fact that sometimes some risks must remain. This chapter focuses on risk and various ways of dealing with it, all of which you will need to understand fully for the Security+ exam.

**Risk Assessment**

Risk assessment is also known as risk analysis. It deals with the threats, vulnerabilities, and impacts of a loss of information-processing capabilities or information itself. Each risk that can be identified should be outlined, described, and evaluated for the likelihood of it occurring. The key is to think out of the box. Conventional threats/risks are often too limited when considering risk assessment.

The key components of a risk-assessment process are outlined here:

**Risks to Which the Organization Is Exposed**  This component allows you to develop scenarios that can help you evaluate how to deal with these risks if they occur. An operating system, server, or application may have known risks in certain environments. You should create a plan for how your organization will best deal with these risks and the best way to respond.

**Risks That Need Addressing**  The risk-assessment component also allows an organization to provide a reality check on which risks are real and which aren’t likely. This process helps an organization focus on its resources as well as on the risks that are most likely to occur. For example, industrial espionage and theft are likely, but the risk of a pack of wild dogs stealing the entire contents of the payroll file is very low. Therefore, resources should be allocated to prevent espionage or theft as opposed to the latter possibility.

**Coordination with BIA**  The risk-assessment component, in conjunction with the BIA (Business Impact Analysis) which is discussed in Chapter 13, provides an organization
with an accurate picture of the situation facing it. It allows an organization to make intelligent decisions about how to respond to various scenarios.

**Real World Scenario**

**Conducting a Risk Assessment**

You’ve been asked to do a quick assessment of the risks your company faces from a security perspective. What steps might you take to develop an overview of your company’s problems?

1. Interview the department heads and the owners to determine what information they feel needs additional security and what the existing vulnerabilities are from their perspectives.

2. Evaluate the servers to determine their known vulnerabilities and how you might counter them.

3. Make sure you do a physical assessment of the facility to evaluate what physical risks you must counter.

Armed with this information, you have a place to start, and you can determine which measures may be appropriate for the company from a risk perspective.

**Computing Risk Assessment**

When you’re doing a risk assessment, one of the most important things to do is to prioritize. Not everything should be weighed evenly because some events have a greater likelihood of happening; in addition, a company can live with some risks, whereas others would be catastrophic. One method of measurement to consider is *annualized rate of occurrence* (ARO). This is the likelihood, often drawn from historical data, of an event occurring within a year. This measure can be used in conjunction with a monetary value assigned to data to compute *single loss expectancy* (SLE) and *annual loss expectancy* (ALE) values.

When you’re computing risk assessment, remember this formula:

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

Thus, if you can reasonably expect that every SLE, which is equal to asset value (AV) times exposure factor (EF), will be equivalent to $1,000 and that there will be seven occurrences a year (ARO), then the ALE is $7,000. Conversely, if there is only a 10 percent chance of an event occurring in a year (ARO = .1), then the ALE drops to $100.

In Exercise 1.1, we’ll walk through some risk-assessment computations.
Chapter 1 • Measuring and Weighing Risk

Real World Scenario

Risk-Assessment Computations

As a security professional, you should know how to compute SLE, ALE, and ARO. Given any two of the numbers, it’s possible to calculate the third. Following are three separate scenarios detailing a hypothetical risk assessment situation followed by details for how to figure out the ALE. They are intended to give you experience working scenarios similar to those you may find on the Security+ exam. For this exercise, compute the missing values:

1. You’re the administrator of a web server that generates $25,000 per hour in revenue. The probability of the web server failing is estimated to be 25 percent, and a failure would lead to three hours of downtime and cost $5,000 in components to correct. What is the ALE?

   The SLE is $80,000 ($25,000 \times 3 \text{ hours} + $5,000), and the ARO is .25. Therefore the ALE is $20,000 ($80,000 \times .25).

2. You’re the administrator for a research firm that works on only one project at a time and collects data through the Web to a single server. The value of each research project is approximately $100,000. At any given time, an intruder could commandeer no more than 90 percent of the data. The industry average for ARO is .33. What is the ALE?

   The SLE equals $90,000 ($100,000 \times .9), and the ARO is .33. Therefore, the ALE is $29,700 ($90,000 \times .33).

3. You work at the help desk for a small company. One of the most common requests you must respond to is to help retrieve a file that has been accidentally deleted by a user. On average, this happens once a week. If the user creates the file and then deletes it on the server (about 60 percent of the incidents), then it can be restored in moments from the shadow copy, and there is rarely any data lost. If the user creates the file on their workstation and then deletes it (about 40 percent of the incidents), and if it can’t be recovered and it takes the user an average of two hours to re-create it at $12 an hour, what is the ALE?

   The SLE is $24 ($12 \times 2), and the ARO is 20.8 (52 weeks \times .4). Therefore the ALE equals $499.20 ($24 \times 20.8).

Key to any risk assessment is identifying both assets and threats. You first have to identify what you want to protect and then what possible harms could come to those assets. You then analyze the risks in terms of either cost or severity.

Risk assessment can be either qualitative (opinion-based and subjective) or quantitative (cost-based and objective), depending upon whether you are focusing on dollar amounts or not. The formulas for single loss expectancy (SLE), annual loss expectancy (ALE), and annualized rate of occurrence (ARO) are all based on doing assessments that lead to dollar amounts and are thus quantitative.
To understand the difference between quantitative and qualitative, it helps to use a simplistic example. Imagine that you get an emergency call to help a small company that you have never even heard from before. It turns out that their one and only server has crashed and their backups are useless. One of the files lost was the only copy of the company history. This file detailed the company from the day it began to the present day and had the various iterations of the mission statement as they changed over time. As painful a loss as this file represents to the company culture, it has nothing to do with filling orders and keeping customers happy and its loss represents a qualitative loss.

Another loss was the customer database. This held customer contact information as well as a history of all past orders, charge numbers, and so on. The company cannot function without this file and it needs to be re-created by pulling all the hard copy invoices from storage and re-entering them into the system. This loss can be calculated by the amount of business lost and the amount of time it takes to find/re-enter all the data, and thus it is a quantitative loss.

**Acting on Your Risk Assessment**

Once you've identified and assessed the risks that exist, for the purpose of the exam, you have five possible actions you can choose to follow:

**Risk Avoidance**  *Risk avoidance* involves identifying a risk and making the decision to no longer engage in the actions associated with that risk. For example, a company could decide that many risks are associated with email attachments and choose to forbid any email attachments from entering the network.

**Risk Transference**  *Risk transference*, contrary to what the name may imply, does not mean that you shift the risk completely to another entity. What you do instead is share some of the burden of the risk with someone else, such as an insurance company. A typical policy would pay you a cash amount if all the steps were in place to reduce risk and your system still was harmed.

**Risk Mitigation**  *Risk mitigation* is accomplished anytime you take steps to reduce the risk. This category includes installing antivirus software, educating users about possible threats, monitoring the network traffic, adding a firewall, and so on. In Microsoft’s Security Intelligence Report, Volume 9, they list the following suggestions for mitigating risk:

- Keep security messages fresh and in circulation.
- Target new employees and current staff members.
- Set goals to ensure a high percentage of the staff is trained on security best practices.
- Repeat the information to raise awareness.

**Risk Deterrence**  *Risk deterrence* involves understanding something about the enemy and letting them know the harm that can come their way if they cause harm to you. This can be as simple as posting prosecution policies on your login pages and convincing them that you have steps in place to identify intrusions and act on them.

**Risk Acceptance**  *Risk acceptance* is often the choice you must make when the cost of implementing any of the other four choices exceeds the value of the harm that would occur
if the risk came to fruition. To truly qualify as acceptance, it cannot be a risk that the administrator/management does not know exists; it has to be an identified risk for which those involved understand the potential cost/damage and agree to accept.

It can often be helpful to create sagacious examples to help in understanding or memorizing various lists, and this works well for the five possible risk actions. Imagine that you are a junior administrator for a large IT department and you believe that one of the older servers should be replaced with a new one. There are no signs of failure now, but it would be prudent to upgrade before anything disastrous happens. The problem, however, is that all spending requires approval from your superior, who is focused on saving the company as much money as possible in order to be considered for a promotion, and he does not want anyone finding ways to spend money. You know him well enough to fear that if a problem does occur, he will not hesitate to put all the blame on you in order to save his own career. Table 1.1 shows how you would apply each of the possible risk actions to this scenario.

**Table 1.1** Risk actions for the scenario

<table>
<thead>
<tr>
<th>Risk Action</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk avoidance</td>
<td>You begin moving services from the older server to other servers and remove the load to avoid the risk of any services being affected by its demise.</td>
</tr>
<tr>
<td>Risk transference</td>
<td>You write up the possibility of the server failing along with details of what you think should be done to prevent it and submit it to your boss while keeping a copy for yourself. If the server does fail, you have proof that you documented this possibility and made the appropriate parties aware of the situation.</td>
</tr>
<tr>
<td>Risk mitigation</td>
<td>You write up the possibility of failure and submit it to your boss while also moving crucial services from that server to others.</td>
</tr>
<tr>
<td>Risk deterrence</td>
<td>You write up the possibility of the server failing along with details of what you think should be done to prevent it and submit it not only to your boss but also to his boss. Use quantitative analysis to show the logic in replacing the server before it fails rather than after.</td>
</tr>
<tr>
<td>Risk acceptance</td>
<td>You know the server could fail but pray that it doesn’t. You don’t write and submit reports because you don’t want to rock the boat and make your boss unhappy with you. With luck, you’ll have transferred to coding before the server ever goes down.</td>
</tr>
</tbody>
</table>
Risks Associated with Cloud Computing

The term *cloud computing* has grown in popularity recently, but few agree on what it truly means. For the purpose of the Security+ exam, cloud computing means using the Internet to host services and data instead of hosting it locally. Some examples of this include running Office-like applications from the Web (such as Google Docs) instead of having the applications installed on each workstation, storing data on server space rented from Amazon, using sites such as Salesforce.com, and so on.

From an exam standpoint, there are three ways of implementing cloud computing:

**Platform as a Service**  The Platform as a Service (PaaS) model is also known as cloud platform services. In this model, vendors allow apps to be created and run on their infrastructure. Two well-known models of this implementation are Amazon Web Services and Google Code.

**Software as a Service**  The Software as a Service (SaaS) model is the one often thought of when users generically think of cloud computing. In this model, applications are remotely run over the Web. The big advantage is that no local hardware is required (other than to obtain web access) and no software applications need be installed on the machine accessing the site. The best known model of this is Salesforce.com. Costs are usually computed on a subscription basis.

**Infrastructure as a Service**  The Infrastructure as a Service (IaaS) model utilizes virtualization, and clients pay an outsourcer for resources used. Because of this, this model closely resembles the traditional utility model used by electric, gas, and water providers. GoGrid is a well-known example of this implementation.

A number of organizations have examined risk-related issues that can be associated with cloud computing. These issues include the following:

**Regulatory Compliance**  Depending upon the type and size of your organization, there are any number of regulatory agency’s rules with which you must comply. If your organization is publically traded, for example, then you must adhere to Sarbanes-Oxley’s demanding and exacting rules—which can be difficult to do when the data is not located on your servers. Make sure whoever hosts your data takes privacy and security as seriously as you do.

**User Privileges**  Enforcing user privileges can be fairly taxing. If the user does not have least privilege (addressed later in this chapter), then their escalated privileges could allow them to access data they otherwise would not be able to and cause harm to it, whether intentional or not. Be cognizant of the fact that you won’t have the same control over user accounts in the cloud as you did locally, and when someone locks their account by giving the wrong password too many times in a row, you/they could be at the mercy of the hours the technical staff is available at the provider.

**Data Integration/Segregation**  Just as web-hosting companies usually put more than one company’s website on a server in order to be profitable, data-hosting companies can put more than one company’s data on a server. In order to keep this from being problematic, you should use encryption to protect your data. Be cognizant of the fact that your data is
only as safe as the data it is integrated with. As an overly simplistic example, assume that your client database is hosted on a server that another company is also using to test an application they are creating. If their application obtains root level at some point (such as to change passwords) and crashes at that point, then the user running the application could be left with root permissions and conceivably be able to see data on the server beyond what they should see (such as your client database). Data segregation is crucial; keep your data on secure servers.

Data integration is equally important—making certain your data is not comingled beyond your expectations. It is not uncommon in an extranet to pull information from a number of databases in order to create a report. Those databases can be owned by anyone connected to the extranet, and it is important to make certain the permissions on your databases are set properly to keep other members from accessing more information that you intended to share.

Among the groups focused on cloud security issues, one worth paying attention to is the Cloud Security Alliance (http://www.cloudsecurityalliance.org). As of this writing, they have published “Top Threats to Cloud Computing” and “Security Guidance for Critical Areas of Focus in Cloud Computing,” which are both highly recommended reading for security administrators.

Risks Associated with Virtualization

If cloud computing has grown in popularity, virtualization has become the technology du jour. Virtualization—allowing one set of hardware to host multiple virtual machines—is in use at most large corporations and becoming more common at smaller businesses as well.

Some of the security risks that are possible with virtualization include the following:

Breaking Out of the Virtual Machine If a malcontent could break out of the virtualization layer and be able to access the other virtual machines, they could access data they should never have access to.

Network and Security Controls Can Intermingle The tools used to administer the virtual machine may not have the same granularity as those used to manage the network. This could lead to privilege escalation and a compromise of security.

Most virtualization-specific threats focus on the hypervisor. The hypervisor is the virtual machine monitor—the software that allows the virtual machines to exist. If the hypervisor can be successfully attacked, the attacker can gain root-level access to all virtual systems. While this is a legitimate issue, and one that has been demonstrated to be possible in most systems (including VMware, Xen, and Microsoft Virtual Machine), it is one that has been patched each time it has reared. The solution to most virtualization threats is to always apply the most recent patches and keep the system(s) up to date.
Developing Policies, Standards, and Guidelines

The process of implementing and maintaining a secure network must first be addressed from a policies, standards, and guidelines perspective. This sets the tone, provides authority, and gives your efforts the teeth they need to be effective. Policies and guidelines set a standard of expectation in an organization. The process of developing these policies will help everyone in an organization become involved and invested in making security efforts successful. You can think of policies as providing the big picture on issues. Standards tell people what is expected, and guidelines provide specific advice on how to accomplish a given task or activity.

The next sections discuss the policies, standards, and guidelines you need to establish in order for your security efforts to be successful.

Implementing Policies

Policies provide the people in an organization with guidance about their expected behavior. Well-written policies are clear and concise, and they outline consequences when they aren’t followed. A good policy contains several key areas besides the policy itself:

- **Scope Statement**  — A good policy has a scope statement that outlines what the policy intends to accomplish and which documents, laws, and practices the policy addresses. The scope statement provides background to help readers understand what the policy is about and how it applies to them.

- **Policy Overview Statement**  — A policy overview statement provides the goal of the policy, why it’s important, and how to comply with it. Ideally, a single paragraph is all you need to provide readers with a sense of the policy.

- **Policy Statement**  — Once the policy’s readers understand its importance, they should be informed of what the policy is. A policy statement should be as clear and unambiguous as possible. The policy may be presented in paragraph form, as bulleted lists, or as checklists.
Chapter 1 • Measuring and Weighing Risk

The presentation will depend on the policy’s target audience as well as its nature. If the policy is intended to help people determine how to lock up the building at the end of the business day, for example, it might be helpful to provide a specific checklist of the steps that should be taken.

**Accountability Statement** The policy should address who is responsible for ensuring that it is enforced. This statement provides additional information to the reader about who to contact if a problem is discovered. It should also indicate the consequences of not complying with the policy.

The accountability statement should be written in words the reader can understand. If the accountability statement is to be read by the users, then it must be written in such a way as to leave no room for misinterpretation.

**Exception Statement** Sometimes even the best policy doesn’t foresee every eventuality. The exception statement provides specific guidance about the procedure or process that must be followed in order to deviate from the policy. This may include an escalation contact, in the event that the person dealing with a situation needs to know whom to contact.

The policy development process is sometimes time consuming. The advantage of this process, though, is that the decisions can be made in advance and can be sent to all involved parties so the policy doesn’t have to be restated over and over again. In fact, formally developing policies saves time and provides structure: Instead of using valuable time trying to figure out what to do, employees will know what to do.

**Incorporating Standards**

A standard deals with specific issues or aspects of a business. Standards are derived from policies. A standard should provide enough detail that an audit can be performed to determine if the standard is being met. Standards, like policies, have certain structural aspects in common.

The following five points are the key aspects of standards documents:

**Scope and Purpose** The standards document should explain or describe the intention. If a standard is developed for a technical implementation, the scope might include software, updates, add-ins, and any other relevant information that helps the implementer carry out the task.

**Roles and Responsibilities** This section of the standards document outlines who is responsible for implementing, monitoring, and maintaining the standard. In a system configuration, this section would outline what the customer is supposed to accomplish and what the installer is supposed to accomplish. This doesn’t mean that one or the other can’t exceed those roles; it means that in the event of confusion, it’s clear who is responsible for accomplishing which tasks.

**Reference Documents** This section of the standards document explains how the standard relates to the organization’s different policies, thereby connecting the standard to
Developing Policies, Standards, and Guidelines

the underlying policies that have been put in place. In the event of confusion or uncertainty, it also allows people to go back to the source and figure out what the standard means. You’ll encounter many situations throughout your career where you’re given a standard that doesn’t make sense. Frequently, by referring to the policies, you can figure out why the standard was written the way it was. Doing so may help you carry out the standard or inform the people responsible for the standard of a change or problem.

**Performance Criteria**  This part of the standards document outlines how to accomplish the task. It should include relevant baseline and technology standards. Baselines provide a minimum or starting point for the standard. Technology standards provide information about the platforms and technologies. Baseline standards spell out high-level requirements for the standard or technology.

| Tip | An important aspect of performance criteria is benchmarking. You need to define what will be measured and the metrics that will be used to do so. |

If you’re responsible for installing a server in a remote location, for example, the standards spell out what type of computer will be used, what operating system will be installed, and any other relevant specifications.

**Maintenance and Administrative Requirements**  These standards outline what is required to manage and administer the systems or networks. For instance, in the case of a physical security requirement, the frequency with which locks or combinations are changed would be addressed.

As you can see, the standards documents provide a mechanism for both new and existing standards to be evaluated for compliance. The process of evaluation is called an *audit*. Increasingly, organizations are being required to conduct regular audits of their standards and policies.

**Following Guidelines**

*Guidelines* are slightly different from either policies or standards. Guidelines help an organization implement or maintain standards by providing information on how to accomplish the policies and maintain the standards.

Guidelines can be less formal than policies or standards because their nature is to help users comply with policies and standards. An example might be an explanation of how to install a service pack and what steps should be taken before doing so.

Guidelines aren’t hard-and-fast rules. They may, however, provide a step-by-step process to accomplish a task. Guidelines, like standards and policies, should contain background information to help a user perform the task.

The following four items are the minimum contents of a good guidelines document:

**Scope and Purpose**  The scope and purpose provide an overview and statement of the guideline’s intent. It is not uncommon to see the heading “Purpose and Scope” or “Scope and Purpose” at the beginning of a document followed by verbiage to the effect: “This
document contains the guidelines and procedures for the assignment and use of xyz and establishes the minimum requirements for governing the acceptable use of…”

Where the scope and purpose are two separate headings, the information beneath the “Purpose” section states why it exists (i.e., “This policy establishes guidelines and minimum requirements governing…”) and the “Scope” section tells who it applies to (i.e., “This policy applies to any employee who…”).

Roles and Responsibilities  This section of the guidelines identifies which individuals or departments are responsible for accomplishing specific tasks. This may include implementation, support, and administration of a system or service. In a large organization, it’s likely that the individuals involved in the process will have different levels of training and expertise. From a security perspective, it could be disastrous if an unqualified technician installed a system without guidelines.

Guideline Statements  These statements provide the step-by-step instructions on how to accomplish a specific task in a specific manner. Again, these are guidelines—they may not be hard-and-fast rules.

Operational Considerations  A guideline’s operational considerations specify and identify what duties are required and at what intervals. This list might include daily, weekly, and monthly tasks. Guidelines for systems backup, for example, might provide specific guidance as to which files and directories must be backed up and how frequently.

Guidelines help an organization in three different ways. First, if a process or set of steps isn’t performed routinely, experienced support and security staff will forget how to do them; guidelines will help refresh their memory. Second, when you’re trying to train someone to do something new, written guidelines can improve the new person’s learning curve. Third, when a crisis or high-stress situation occurs, guidelines can keep you from coming unglued.

Business Policies

Business policies also affect the security of an organization. They address organizational and departmental business issues as opposed to corporate-wide personnel issues. When developing your business policy, you must consider these primary areas of concern:

- Separation of duties
- Due care
- Physical access control
- Document disposal and destruction
- Privacy policy
- Acceptable use
- Security policy
- Mandatory vacations
- Job rotation
- Least privilege

The following sections discuss these areas.
Separation of Duties Policies

Separation of duties policies are designed to reduce the risk of fraud and prevent other losses in an organization. A good policy will require more than one person to accomplish key processes. This may mean that the person who processes an order from a customer isn’t the same person who generates the invoice or deals with the billing.

Separation of duties helps prevent various problems, such as an individual embezzling money from a company. To successfully embezzle funds, an individual would need to recruit others to commit an act of collusion (an agreement between two or more parties established for the purpose of committing deception or fraud). Collusion, when part of a crime, is also a criminal act in and of itself.

In addition, separation-of-duties policies can help prevent accidents from occurring in an organization. Let’s say you’re managing a software development project. You want someone to perform a quality assurance test on a new piece of code before it’s put into production. Establishing a clear separation of duties prevents development code from entering production status until quality testing is accomplished.

Many banks and financial institutions require multiple steps and approvals to transfer money. This helps reduce errors and minimizes the likelihood of fraud.

Very small attacks are often called salami attacks. In banking, various forms of salami attacks can occur, such as shaving a few cents from many accounts, rounding to whole numbers and compiling the remainder into one account, and so on.

Due Care Policies

Due care policies identify the level of care used to maintain the confidentiality of private information. These policies specify how information is to be handled. The objectives of due care policies are to protect and safeguard customer and/or client records. The unauthorized disclosure of this information creates a strong potential for liability and lawsuits. Everyone in an organization must be aware of and held to a standard of due care with confidential records.

It’s easy to say that everyone else should adhere to policies and then overlook the importance of doing so yourself. As an administrator, you have access to a great deal of personal information, and you need to be as careful with it, if not more careful, as anyone else in the organization. In many cases, something as simple as a printed list of user information sitting in plain view on your desk can violate rules of disclosure.

One of the leading ways to handle due care policies is to implement best practices. Best practices are based on what is known in the industry and how others would respond to similar situations.
Physical Access Control Policies

Physical access control policies refer to the authorization of individuals to access facilities or systems that contain information. Implementing a physical access control policy helps prevent theft and unauthorized disclosure of information and keeps other problems from cropping up. Many organizations limit office hours of employees to prevent them from accessing computer systems during odd hours. (This may not be appropriate for some positions, but it may be essential in others.) What would happen in your company if a payroll clerk decided to give herself a raise? In all probability, she wouldn’t do this under the supervision of the payroll manager—she would do it when no one was around. By limiting access to the physical premises and computer systems, you reduce the likelihood that an individual will be tempted to commit a crime.

Document Disposal and Destruction Policies

Document disposal and destruction policies define how information that is no longer needed is handled. According to Microsoft’s Security Intelligence Report, Volume 9, “Improper disposal of business records is the second largest source of breach incidents related to negligence, and the third largest source of incidents overall.”

You should ensure that financial, customer, and other sensitive information is disposed of properly when it’s no longer needed. Most organizations use mountains of paper, and much of it needs to be shredded or destroyed to prevent unauthorized access to sensitive information. Investigate the process that your organization uses to dispose of business records; it may need to be reevaluated.

Many large cities have businesses that do nothing but destroy paper for banks and other institutions. Using a truck that resembles a mobile shredder on wheels, they will come to your site and guarantee that the paper is destroyed. If your organization works with data of a sensitive nature, you should investigate the possibility of using such a service.

Privacy Policies

Privacy policies define what controls are required to implement and maintain the sanctity of data privacy in the work environment. Many of the restrictions regarding privacy are addressed in legislation and covered in Chapter 6. For now, however, think of the privacy policy as a legal document that outlines how data collected is secured. A great example of a privacy policy is Google’s (see http://www.google.com/privacy/privacy-policy.html), which outlines exactly what information the company collects, choices you have based on your account, information sharing of the data that is done with other parties, security measure in place, and enforcement. The last paragraph of the policy should appear in every policy and addresses the fact that the policy may change. The verbiage, as currently written, is succinct and clear: “Please note that this Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any Privacy Policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.”
Acceptable Use Policies

Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources: both software and hardware. This policy should also outline the consequences for misuse. In addition, the policy (also known just as a use policy) should address installation of personal software on company computers and the use of personal hardware such as USB devices. When portable devices are plugged directly into a machine, they bypass the network security measures (such as firewalls) and allow data to be copied in what is known as pod slurping.

Even secure workstations that contain no traditional media devices (CD, DVD, and so forth) usually contain USB ports. Unless those ports are disabled, a user can easily connect a flash drive and copy files to and from it. Not only should you make every attempt to limit USB ports, but you should also have the use of such devices spelled out in the acceptable use policy to circumvent the “I didn’t know” defense.

Real World Scenario

The Trouble with Not Having a Policy

A few years ago, an employee in a large company was using corporate computer systems to run a small accounting firm he had started. He was using the computers on his own time. When this situation was discovered, he was immediately fired for the misuse of corporate resources. He sued the company for wrongful discharge and won the case. The company was forced to hire him back and pay his back wages, and he was even awarded damages. The primary reason the company lost the case was that its acceptable use policy didn’t say he couldn’t use the company computers for personal work, only that he couldn’t use them for personal work during work hours. The company wasn’t able to prove that he did the personal work during work hours.

Every acceptable use policy today should include a section on cell phone usage (and even presence) within the workplace. While a cell phone can be convenient for employees (they can now more easily take personal calls at work), it can be a headache for the security administrator. Most cell phones can store files the same as any USB device and can be used to copy files to and from the workstation. Additionally, the camera feature of most phones makes it possible for a user to take pictures of such things as documents, your servers, your physical security implementation, and many other things you probably don’t want to share. For this reason, most secure facilities have stringent restrictions on the presence of cell phones within the vicinity.

Make sure your acceptable use policies provide you with adequate coverage regarding all acceptable uses of corporate resources.
Security Policies

Security policies define what controls are required to implement and maintain the security of systems, users, and networks. This policy should be used as a guide in system implementations and evaluations. Security policies will be discussed throughout the book, and you should be aware of their key aspects.

Mandatory Vacations

A mandatory vacation policy requires all users to take time away from work and refresh. As contradictory as it may seem, an employee who doesn’t take their vacation time can be detrimental to the health not only of the employee but of the company as well. If the company becomes too dependent on one person, they can end up in a real bind if something should happen to that person. Not only does the mandatory vacation give the employee a chance to refresh, but it also gives the company the chance to make sure others can fill in any gaps in skills and satisfy the need to have replication/duplication at all levels. The mandatory vacations also provide an opportunity to discover fraud.

Job Rotation

A job rotation policy defines intervals at which employees must rotate through positions. Similar in purpose to mandatory vacations, it helps to ensure that the company does not become too dependent on one person (who then has the ability to do enormous harm). Rotate jobs on a frequent enough basis so that you are not putting yourself—and your data—at the mercy of any one administrator. Just as you want redundancy in hardware, you want redundancy in abilities.

When one person fills in for another, such as for mandatory vacations, it provides an opportunity to see what the person is doing and potentially uncover any fraud.

Least Privilege

A least privilege policy should be used when assigning permissions. Give users only the permissions they need to do their work and no more. For example, a temporary employee should never have the right to install software, a receptionist does not need the right to make backups, and so on. Every operating system includes the ability to limit users based on groups and individual permissions, and your company should adhere to the policy of always applying only those permissions users need and blocking all others.

Understanding Control Types, False Positives, and Change and Incident Management

Risk assessment/analysis involves calculating potential risks and making decisions based on the variables associated with those risks (likelihood, ALE, impact, etc.). Once you’ve identified risks that you want to address with actions other than avoidance, you put controls in place to address the risks.

The U.S. Department of Energy Cyber Security Program places controls into various types. The control types fall into three categories: Management, Operational, and
Technical, as defined in the Management, Operational, and Technical Controls Guidance (http://www.ornl.gov/doe/doe_oro_dmg/TMR/TMRs/CS01%20Final%20Controls%20070706.pdf). Table 1.2 shows the various controls and the classification type they fall under.

While risk assessment was discussed in this chapter, most of the other controls are addressed in subsequent chapters.

**TABLE 1.2** Control Types and Controls

<table>
<thead>
<tr>
<th>Control Type</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Management</td>
<td>Planning</td>
</tr>
<tr>
<td>Management</td>
<td>System and Services Acquisition</td>
</tr>
<tr>
<td>Management</td>
<td>Certification, Accreditation, and Security Assessment</td>
</tr>
<tr>
<td>Operational</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>Operational</td>
<td>Physical and Environmental Protection</td>
</tr>
<tr>
<td>Operational</td>
<td>Contingency Planning</td>
</tr>
<tr>
<td>Operational</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>Operational</td>
<td>Maintenance</td>
</tr>
<tr>
<td>Operational</td>
<td>System and Information Integrity</td>
</tr>
<tr>
<td>Operational</td>
<td>Media Protection</td>
</tr>
<tr>
<td>Operational</td>
<td>Incident Response</td>
</tr>
<tr>
<td>Operational</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td>Technical</td>
<td>Identification and Authentication</td>
</tr>
<tr>
<td>Technical</td>
<td>Access Control</td>
</tr>
<tr>
<td>Technical</td>
<td>Audit and Accountability</td>
</tr>
<tr>
<td>Technical</td>
<td>System and Communication Protection</td>
</tr>
</tbody>
</table>

After you have implemented security controls based on risk, you must routinely perform routine audits. Those audits should include reviews of user rights and permissions as well as events that occur. You should pay particular attention to false positives, change management, and incident management.

False positives are events that aren’t really incidents. Event flagging is often based on established rules of acceptance (deviations from which are known as anomalies) and such things as attack signatures. If the rules aren’t set up properly, normal traffic may set off the analyzer and generate an event. You don’t want to declare an emergency unless you’re sure you have one.

The audits should address change management—the structured approach that is followed to secure the company’s assets—and incident management—the steps followed when events occur. Details here should include the controls that are in place to prevent unauthorized access to, and changes of, all IT assets.

Summary

Risk assessment is the process of evaluating and cataloging the threats, vulnerabilities, and weaknesses that exist in the systems being used. The risk assessment should tie in with BCP to ensure that all bases are covered.

Security models begin with an understanding of the business issues an organization is facing. The following business issues must be evaluated:

- Policies
- Standards
- Guidelines

A good policy design includes scope statements, overview statements, accountability expectations, and exceptions. Each of these aspects of a well-crafted policy helps set the expectation for everyone in a company. For a policy to be effective, it needs the unequivocal support of the senior management or decision makers in an organization.
Know the three categories of control types. The three types of controls that can be administered are Technical, Management, and Operational.

Know how to calculate risk. Risk can be calculated either qualitatively (subjective) or quantitatively (objective). Quantitative calculations assign dollar amounts, and the basic formula is $SLE \times ARO = ALE$ where SLE is the single loss expectancy, ARO is the annualized rate of occurrence, and ALE is the annual loss expectancy.

Know the five different approaches to risk. The five risk strategies are avoidance (don’t engage in that activity), transference (think insurance), mitigation (take steps to reduce the risk), deterrence (warn of harm to others if they affect you), and acceptance (be willing to live with the risk).

Know the importance of policies, standards, and guidelines. The process of implementing and maintaining a secure network must first be addressed from a policies, standards, and guidelines perspective. Policies and guidelines set a standard of expectation in an organization. Standards tell people what is expected, and guidelines provide specific advice on how to accomplish a given task or activity.

Know the principles of cloud computing. Cloud computing can be implemented three ways: Platform as a Service, Software as a Service, and Infrastructure as a Service. Each provides a different set of threats that administrators must be cognizant of.
Review Questions

1. You’re the chief security contact for MTS. One of your primary tasks is to document everything related to security and create a manual that can be used to manage the company in your absence. Which documents should be referenced in your manual as the ones that identify the methods used to accomplish a given task?
   A. Policies
   B. Standards
   C. Guidelines
   D. BIA

2. Consider the following scenario: The asset value of your company’s primary servers is $2 million and they are housed in a single office building in Anderson, Indiana. You have field offices scattered throughout the United States, so the servers in the main office account for approximately half the business. Tornados in this part of the country are not uncommon, and it is estimated one will level the building every 60 years.

   Which of the following is the SLE for this scenario?
   A. $2 million
   B. $1 million
   C. $500,000
   D. $33,333.33
   E. $16,666.67

3. Refer to the scenario in question 2. Which of the following is the ALE for this scenario?
   A. $2 million
   B. $1 million
   C. $500,000
   D. $33,333.33
   E. $16,666.67

4. Refer to the scenario in question 2. Which of the following is the ARO for this scenario?
   A. 0.0167
   B. 1
   C. 5
   D. 16.7
   E. 60
5. Which of the following strategies involves identifying a risk and making the decision to no longer engage in the action?
   A. Risk acceptance
   B. Risk avoidance
   C. Risk deterrence
   D. Risk mitigation
   E. Risk transference

6. Which of the following policy statements may include an escalation contact, in the event that the person dealing with a situation needs to know whom to contact?
   A. Scope
   B. Exception
   C. Overview
   D. Accountability

7. Which of the following policies are designed to reduce the risk of fraud and prevent other losses in an organization?
   A. Separation of duties
   B. Acceptable use
   C. Least privilege
   D. Physical access control

8. What is the term used for events that mistakenly were flagged and aren’t truly events to be concerned with?
   A. Fool’s gold
   B. Non-incidents
   C. Error flags
   D. False positives

9. Which of the following is the structured approach that is followed to secure the company’s assets?
   A. Asset management
   B. Incident management
   C. Change management
   D. Skill management

10. Which of the following strategies involves sharing some of the burden of the risk with someone else such as an insurance company?
    A. Risk acceptance
    B. Risk avoidance
    C. Risk deterrence
    D. Risk mitigation
    E. Risk transference
11. The risk-assessment component, in conjunction with the ________, provides the organization with an accurate picture of the situation facing it.
   A. RAC  
   B. ALE  
   C. BIA  
   D. RMG

12. Which of the following policy statements should address who is responsible for ensuring that it is enforced?
   A. Scope  
   B. Exception  
   C. Overview  
   D. Accountability

13. Which of the following strategies is accomplished anytime you take steps to reduce the risk?
   A. Risk acceptance  
   B. Risk avoidance  
   C. Risk deterrence  
   D. Risk mitigation  
   E. Risk transference

14. If you calculate SLE to be $4,000 and that there will be 10 occurrences a year (ARO), then the ALE is:
   A. $400  
   B. $4,000  
   C. $40,000  
   D. $400,000

15. Which of the following policies describes how the employees in an organization can use company systems and resources, both software and hardware?
   A. Separation of duties  
   B. Acceptable use  
   C. Least privilege  
   D. Physical access control

16. Separation of duties helps prevent an individual from embezzling money from a company. To successfully embezzle funds, an individual would need to recruit others to commit an act of ________ (an agreement between two or more parties established for the purpose of committing deception or fraud).
   A. Misappropriation  
   B. Misuse  
   C. Collusion  
   D. Fraud
17. Which of the following strategies involves understanding something about the enemy and letting them know the harm that can come their way if they cause harm to you?
   A. Risk acceptance
   B. Risk avoidance
   C. Risk deterrence
   D. Risk mitigation
   E. Risk transference

18. If you calculate SLE to be $25,000 and that there will be one occurrence every four years (ARO), then what is the ALE?
   A. $6,250
   B. $12,500
   C. $25,000
   D. $100,000

19. Which of the following policies should be used when assigning permissions, giving users only the permissions they need to do their work and no more?
   A. Separation of duties
   B. Acceptable use
   C. Least privilege
   D. Physical access control

20. Which of the following strategies necessitates an identified risk that those involved understand the potential cost/damage and agree to accept?
   A. Risk acceptance
   B. Risk avoidance
   C. Risk deterrence
   D. Risk mitigation
   E. Risk transference
Answers to Review Questions

1. C. Guidelines help clarify processes to maintain standards. Guidelines tend to be less formal than policies or standards.

2. B. SLE (single loss expectancy) is equal to asset value (AV) times exposure factor (EF). In this case, asset value is $2 million and exposure factor is 1/2.

3. E. ALE (annual loss expectancy) is equal to SLE times the annualized rate of occurrence. In this case, SLE is $1 million and the ARO is 1/60.

4. A. ARO (annualized rate of occurrence) is the frequency (in number of years) the event can be expected to happen. In this case, ARO is 1/60 or 0.0167.

5. B. Risk avoidance involves identifying a risk and making the decision to no longer engage in the actions associated with that risk.

6. B. The exception policy statement may include an escalation contact, in the event that the person dealing with a situation needs to know whom to contact.

7. A. The separation of duties policies are designed to reduce the risk of fraud and prevent other losses in an organization.

8. D. False positives are events that mistakenly were flagged and aren’t truly events to be concerned with.

9. C. Change management is the structured approach that is followed to secure the company’s assets.

10. E. Risk transference involves sharing some of the burden of the risk with someone else such as an insurance company.

11. C. The risk-assessment component, in conjunction with the BIA (Business Impact Analysis), provides the organization with an accurate picture of the situation facing it.

12. D. The accountability policy statement should address who is responsible for ensuring that it is enforced.

13. D. Risk mitigation is accomplished anytime you take steps to reduce the risk.

14. C. If you calculate SLE to be $4,000 and that there will be 10 occurrences a year (ARO), then the ALE is $40,000 ($4,000 \times 10).

15. B. The acceptable use policies describe how the employees in an organization can use company systems and resources, both software and hardware.

16. C. Collusion is an agreement between two or more parties established for the purpose of committing deception or fraud. Collusion, when part of a crime, is also a criminal act in and of itself.
17. C. Risk deterrence involves understanding something about the enemy and letting them know the harm that can come their way if they cause harm to you.

18. A. If you calculate SLE to be $25,000 and that there will be one occurrence every four years (ARO), then the ALE is $6,250 ($25,000 \times .25$).

19. C. The principle of least privilege should be used when assigning permissions. Give users only the permissions they need to do their work and no more.

20. A. Risk acceptance necessitates an identified risk that those involved understand the potential cost/damage and agree to accept.