PART ONE

Risk Management Business Challenges

CHAPTER

1 Risk Management Fundamentals

RISK MANAGEMENT IS IMPORTANT to the success of every company—a company that takes no risks doesn't thrive. On the other hand, a company that ignores risk can fail when a single threat is exploited. Nowadays, information technology (IT) systems contribute to the success of most companies. If you don't properly manage IT risks, they can also contribute to your company's failure.

Effective risk management starts by understanding threats and vulnerabilities. You build on this knowledge by identifying ways to mitigate the risks. Risks can be mitigated by reducing vulnerabilities or reducing the impact of the risk. You can then create different plans to mitigate risks in different areas of the company. A company typically has several risk mitigation plans in place.

This text can help you build a solid foundation in risk management as it relates to information system security. It won't make you an expert. Many of the topics presented in a few paragraphs in this text can fill entire chapters or even entire books. The more you learn, the closer you'll be to becoming the expert whom others seek out to solve their problems.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- What risk is and what its relationship to threat, vulnerability, and loss is
- What the major components of risk to an IT infrastructure are
- What risk management is and how it is important to the organization
- What some risk identification techniques are
- What some risk management techniques are

Chapter 1 Goals

When you complete this chapter, you will be able to:

- Define risk
- Identify the major components of risk
- Describe the relationship among threats, vulnerabilities, and impact
- Define risk management
- Describe risk management's relationship with profitability and survivability
- Explain the relationship between the cost of loss and the cost of risk management
- Describe how risk is perceived by different roles within an organization
- Identify threats
- List the different categories of threats
- Describe techniques to identify vulnerabilities
- Identify and define risk management techniques
- Describe the purpose of a cost-benefit analysis (CBA)
- Define residual risk

What Is Risk?

Risk is the likelihood that a loss will occur. Losses occur when a **threat** exposes a **vulnerability**. Organizations of all sizes face risks. Some risks are so severe they cause a business to fail. Other risks are minor and can be accepted without another thought. Companies use risk management techniques to identify and differentiate severe risks from minor risks. When this is done properly, administrators and managers can intelligently decide what to do about any type of risk. The end result is a decision to avoid, share or transfer, mitigate, or accept a risk.

The common themes of these definitions are threat, vulnerability, and loss. Even though the common body of knowledge (CBK) — see note — doesn't specifically mention loss, it implies it. Here's a short definition of each of these terms:

NOTE

The *Official (ISC)² Guide to the SSCP CBK* provides a more technical definition of risk. Risk is "a function of the likelihood of a given threat source's exercising a potential vulnerability, and the resulting impact of that adverse event on the organization." If you're not familiar with the alphabet soup, the (ISC)² System Security Certified Practitioner (SSCP) certification includes seven domains that are derived from a common body of knowledge (CBK).

> **NOTE**
> Threats and vulnerabilities are explored in much more depth later in this chapter.

- **Threat**—A threat is any activity that represents a possible danger.
- **Vulnerability**—A vulnerability is a weakness.
- **Loss**—A loss results in a compromise to business functions or assets.

Risks to a business can result in a loss that negatively affects the business. A business commonly tries to limit its exposure to risks. The overall goal is to reduce the losses that can occur from risk. Some of the risk-related concerns for businesses are:

- Compromise of business functions
- Compromise of business assets
- Driver of business costs
- Profitability versus survivability

Compromise of Business Functions

Business functions are the activities a business performs to sell products or services. If any of these functions are negatively affected, the business won't be able to sell as much. The business will earn less revenue, resulting in an overall loss.

Here are a few examples of business functions and possible compromises:

- Salespeople regularly call or e-mail customers. If the capabilities of either phones or e-mail are reduced, sales are reduced.
- A Web site sells products on the Internet. If the Web site is attacked and fails, sales are lost.
- Authors write articles that must be submitted by a deadline to be published. If the author's PC becomes infected with a virus, the deadline passes and the article's value is reduced.
- Analysts compile reports used by management to make decisions. Data is gathered from internal servers and Internet sources. If network connectivity fails, analysts won't have access to current data. Management could make decisions based on inaccurate information.
- A warehouse application is used for shipping products that have been purchased. It identifies what has been ordered, where the products need to be sent, and where they are located. If the application fails, products aren't shipped on time.

Because compromises to any of these business functions can result in a loss of revenue, they all represent risks. One of the tasks when considering risk is identifying the important functions for a business.

The importance of any business function is relative to the business. In other words, the failure of a Web site for one company may be catastrophic if all products and services are sold through the Web site. Another company may host a Web site to provide information to potential customers. If it fails, it will have less impact on the business.

Compromise of Business Assets

A business asset is anything that has measurable value to a company. If an asset has the potential of losing value, it is at risk. Value is defined as the worth of an asset to a business. Value can often be expressed in monetary terms, such as $5,000.

Assets can have both tangible and intangible values. The **tangible value** is the actual cost of the asset. The **intangible value** is value that cannot be measured by cost, such as client confidence. Generally acceptable accounting principles (GAAP) refer to client confidence as goodwill.

Imagine that your company sells products via a Web site. The Web site earns $5,000 an hour in revenue. Now, imagine that the Web server hosting the Web site fails and is down for two hours. The costs to repair it total $1,000. What is the tangible loss?

- **Lost revenue**—$5,000 times two hours = $10,000
- **Repair costs**—$1,000
- **Total tangible value**—$11,000

The intangible value isn't as easy to calculate but is still very important. Imagine that several customers tried to make a purchase when the Web site was down. If the same product is available somewhere else, they probably bought the product elsewhere. That lost revenue is the tangible value.

However, if the experience is positive with the other business, where will the customers go the next time they want to purchase this product? It's very possible the other business has just gained new customers and you have lost some. The intangible value includes:

- **Future lost revenue**—Any additional purchases the customers make with the other company is a loss to your company.
- **Cost of gaining the customer**—A lot of money is invested to attract customers. It is much easier to sell to a repeat customer than it is to acquire a new customer. If you lose a customer, you lose the investment.
- **Customer influence**—Customers have friends, families, and business partners. They commonly share their experience with others, especially if the experience is exceptionally positive or negative.

Some examples of tangible assets are:

- **Computer systems**—Servers, desktop PCs, and mobile computers are all tangible assets.
- **Network components**—Routers, switches, firewalls, and any other components necessary to keep the network running are assets.

- **Software applications**—Any application that can be installed on a computer system is considered a tangible asset.
- **Data**—This includes the large-scale databases that are integral to many businesses. It also includes the data used and manipulated by each employee or customer.

One of the early steps in risk management is associated with identifying the assets of a company and their associated costs. This data is used to prioritize risks for different assets. Once a risk is prioritized, it becomes easier to identify risk management processes to protect the asset.

Driver of Business Costs

Risk is also a driver of business costs. Once risks are identified, steps can be taken to reduce or manage the risk. Risks are often managed by implementing countermeasures or **controls**. The costs of managing risk need to be considered in total business costs.

If too much money is spent on reducing risk, the overall profit is reduced. If too little money is spent on these controls, a loss could result from an easily avoidable threat and/or vulnerability.

Profitability Versus Survivability

Both **profitability** and **survivability** must be considered when considering risks:

- **Profitability**—The ability of a company to make a profit. Profitability is calculated as revenues minus costs.
- **Survivability**—The ability of a company to survive loss due to a risk. Some losses such as fire can be disastrous and cause the business to fail.

In terms of profitability, a loss can ruin a business. In terms of survivability, a loss may cause a company never to earn a profit. The costs associated with risk management don't contribute directly to revenue gains. Instead, these costs help to ensure that a company can continue to operate even if it incurs a loss.

When considering profitability and survivability, you will want to consider the following items:

- **Out-of-pocket costs**—The cost to reduce risks comes from existing funds.
- **Lost opportunity costs**—Money spent to reduce risks can't be spent elsewhere. This may result in lost opportunities if the money could be used for some other purpose.
- **Future costs**—Some countermeasures require ongoing or future costs. These costs could be for renewing hardware or software. Future costs can also include the cost of employees to implement the countermeasures.
- **Client/stakeholder confidence**—The value of client and stakeholder confidence is also important. If risks aren't addressed, clients or stakeholders may lose confidence when a threat exploits a vulnerability, resulting in a significant loss to the company.

Consider antivirus software. The cost to install antivirus software on every computer in the organization can be quite high. Every dollar spent reduces the overall profit, and antivirus software doesn't have the potential to add any profit.

However, what's the alternative? If antivirus software is not installed, every system represents a significant risk. If any system becomes infected, a virus could release a worm as a payload and infect the entire network. Databases could be corrupted. Data on file servers could be erased. E-mail servers could crash. The entire business could grind to a halt. If this happens too often or for too long, the business could fail.

What Are the Major Components of Risk to an IT Infrastructure?

When you start digging into risk and risk management, you'll realize there is a lot to consider. Luckily, there are several methods and techniques used to break down the topics into smaller chunks.

One method is to examine the seven domains of a typical IT infrastructure. You can examine risks within each domain separately. When examining risks for any domain, you'll look at threats, vulnerabilities, and impact. The following sections explore these topics.

Seven Domains of a Typical IT Infrastructure

There are a lot of similarities between different IT organizations. For example, any IT organization will have users and computers. There are seven domains of a typical IT infrastructure.

Figure 1-1 shows the seven domains of a typical IT infrastructure. Refer to this figure when reading through the descriptions of these domains.

When considering risk management, you can examine each of these domains separately. Each domain represents a possible target for an attacker. Some attackers have the skill and aptitude to con users, so they focus on the User Domain. Other attackers may be experts in specific applications, so they focus on the System/Application Domain.

An attacker only needs to be able to exploit vulnerabilities in one domain. However, a business must provide protection in each of the domains. A weakness in any one of the domains can be exploited by an attacker even if the other six domains have no vulnerabilities.

User Domain

The User Domain includes people. They can be users, employees, contractors, or consultants. The old phrase that a chain is only as strong as its weakest link applies to IT security too. People are often the weakest link in IT security.

You could have the strongest technical and physical security available. However, if personnel don't understand the value of security, the security can be bypassed. For example, technical security can require strong, complex passwords that can't be easily cracked. However, a social engineer can convince an employee to give up the password. Additionally, users may simply write their password down. Some users assume that no one will ever think of looking at the sticky note under their keyboard.

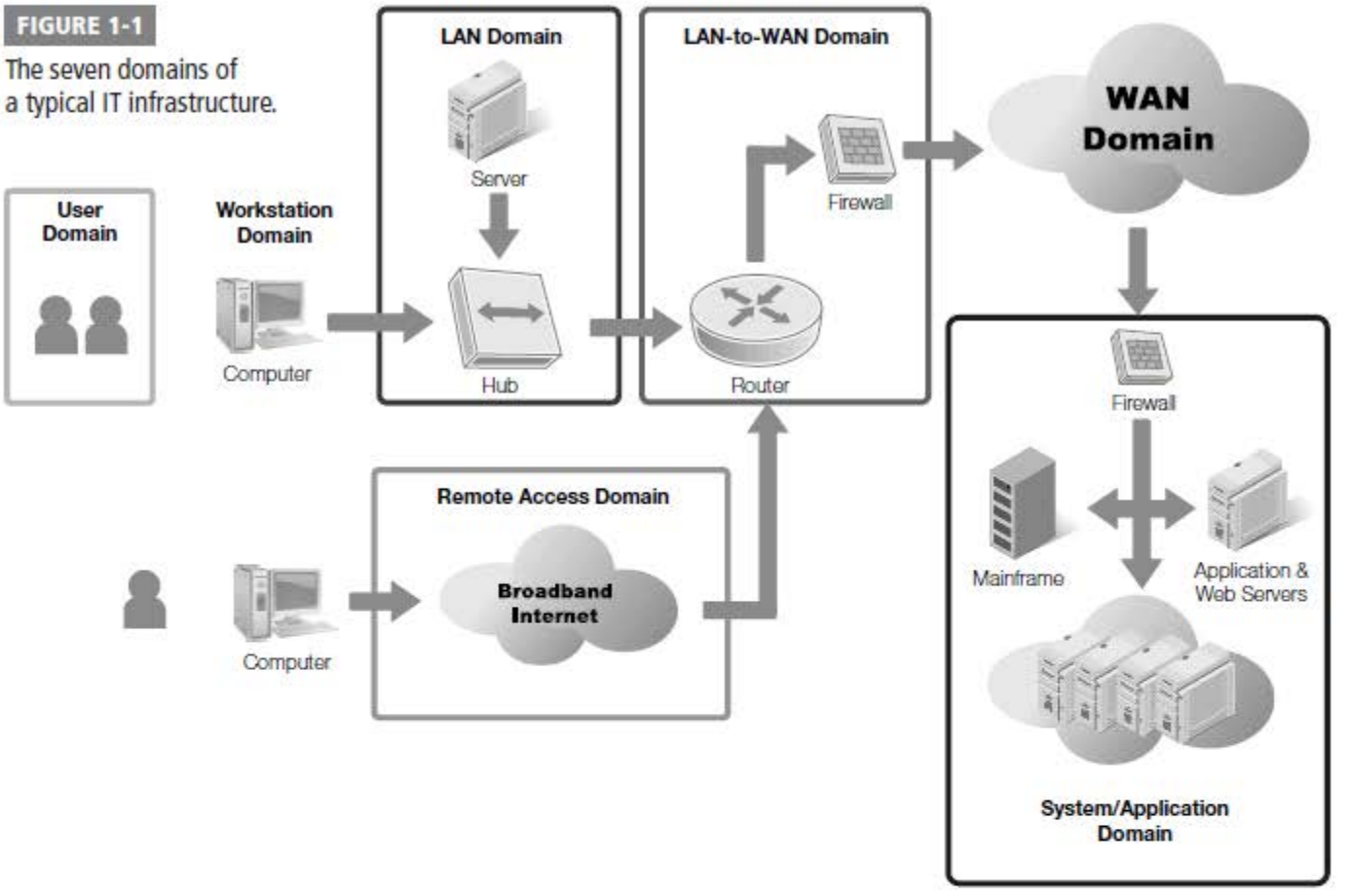


FIGURE 1-1
The seven domains of a typical IT infrastructure.

Users can visit risky Web sites and download and execute infected software. They may unknowingly bring viruses from home via universal serial bus (USB) thumb drives. When they plug in the USB drive, the work computer becomes infected. This in turn can infect other computers and the entire network.

Workstation Domain

The workstation is the end user's computer. The workstation is susceptible to malicious software, also known as *malware*. If antivirus software isn't installed, the workstation is vulnerable. The workstation is also vulnerable if it is not kept up to date with recent patches.

Some malware infects a single system. Other malware releases worm components that can spread across the network.

Antivirus companies regularly update virus definitions as new malware is discovered. In addition to installing the antivirus software, companies must also update software regularly with new definitions. If the antivirus software is installed and up to date, the likelihood of a system becoming infected is reduced.

Bugs and vulnerabilities are constantly being discovered in operating systems and applications. Some of the bugs are harmless. Others represent significant risks.

Demystifying Social Engineering

Social engineering is a common technique used to trick people into revealing sensitive information. Leonardo DiCaprio played Frank Abagnale in the movie *Catch Me If You Can*, which demonstrated the power of social engineering. A social engineer doesn't just say "give me your secrets." Instead, the attacker uses techniques such as flattery and conning.

A common technique used in vulnerability assessments is to ask employees to give their usernames and passwords. The request may come in the form of an e-mail, a phone call, or even person-to-person.

One common method used in vulnerability assessments is to send an e-mail requesting usernames and passwords. The e-mail is modified so that it looks as if it's coming from an executive. The e-mail adds a sense of urgency and may include a reference to an important project. For example, the users might receive the following e-mail:

From: CEO

Subj: Project upgrade

All,

The XYZ project is at risk of falling behind. As you know this is integral to our success in the coming year. We're having a problem with user authentication. We think it's because passwords may have special characters that aren't recognized.

I need everyone to reply to this e-mail with your username and password. We must complete this test today, so please respond as soon as you receive this e-mail.

Thanks for your assistance.

When employees are trained to protect their passwords, they usually recognize the risks and don't reply. However, it has been shown that when employees aren't trained, as many as 70 percent of the employees may respond.

Microsoft and other software vendors regularly release patches and fixes that can be applied. When systems are kept updated, these fixes help keep the systems protected. When systems aren't updated, the threats can become significant.

LAN Domain

The LAN Domain is the area that is inside the firewall. It can be a few systems connected together in a small home office network. It can also be a large network with thousands of computers. Each individual device on the network must be protected or all devices can be at risk.

Network devices such as hubs, switches, and routers are used to connect the systems together on the local area network (LAN). The internal LAN is generally considered a trusted zone. Data transferred within the LAN isn't protected as thoroughly as if it were sent outside the LAN.

> **NOTE**
> Many organizations outlaw the use of hubs within the LAN. Switches are more expensive. However, they reduce the risk of sniffing attacks.

As an example, sniffing attacks occur when an attacker uses a protocol analyzer to capture data packets. A protocol analyzer is also known as a sniffer. An experienced attacker can read the actual data within these packets.

When hubs are used instead of switches, there is an increased risk of sniffing attacks. An attacker can plug into any port in the building and potentially capture valuable data.

When switches are used instead of hubs, the attacker must have physical access to the switch to capture the same amount of data. Most organizations protect network devices in server rooms or wiring closets.

LAN-to-WAN Domain

The LAN-to-WAN Domain connects the local area network to the wide area network (WAN). The LAN Domain is considered a trusted zone because it is controlled by a company. The WAN Domain is considered an untrusted zone because it is not controlled and is accessible by attackers.

The area between the trusted and untrusted zones is protected with one or more firewalls. This is also called the boundary, or the edge. Security here is referred to as boundary protection or edge protection.

The public side of the boundary is often connected to the Internet and has public Internet Protocol (IP) addresses. These IP addresses are accessible from anywhere in the world, and attackers are constantly probing public IP addresses. They look for vulnerabilities and when one is found, they pounce. Because of this, the Internet is an untrusted zone.

A high level of security is required to keep the LAN-to-WAN Domain safe.

Remote Access Domain

Mobile workers often need access to the private LAN when they are away from the company. Remote access is used to grant mobile workers this access. Remote access can be granted via direct dial-up connections or by using a virtual private network (VPN) connection.

A VPN provides access to a private network over a public network. The public network used by VPNs is most commonly the Internet. Since the Internet is largely untrusted and has known attackers, remote access represents a risk. Attackers can access unprotected connections. They can also try to break into the remote access servers. Using a VPN is an example of a control to lessen the risk. But VPNs have their vulnerabilities, too.

Vulnerabilities exist at two stages of the VPN connection:

- The first stage is authentication. Authentication is when the user provides credentials to prove identity. If these credentials can be discovered, the attacker can later use them to impersonate the user.
- The second stage is when data is passed between the user and the server. If the data is sent in cleartext, an attacker can capture and read the data.

> **NOTE**
> VPN connections use tunneling protocols to reduce the risk of data being captured. A tunneling protocol encrypts the traffic sent over the network. This makes it more difficult for attackers to capture and read data.

WAN Domain

For many businesses, the WAN is the Internet. However, a business can also lease semiprivate lines from private telecommunications companies. These lines are semiprivate because they are rarely leased and used by only a single company. Instead, they are shared with other companies.

As mentioned in the "LAN-to-WAN Domain" section, the Internet is an untrusted zone. Any host on the Internet with a public IP address is at significant risk of attack. Moreover, it is fully expected that any host on the Internet will be attacked.

Semiprivate lines aren't as easily accessible as the Internet. However, a company rarely knows who else is sharing the lines. These leased lines require the same level of security provided to any host in the WAN Domain.

A significant amount of security is required to keep hosts in the WAN Domain safe.

System/Application Domain

The System/Application Domain refers to servers that host server-level applications. Mail servers receive and send e-mail for clients. Database servers host databases that are accessed by users, applications, or other servers. Domain Name System (DNS) servers provide names to IP addresses for clients.

You should always protect servers using best practices. Remove unneeded services and protocols. Change default passwords. Regularly patch and update the server systems. Enable local firewalls.

One of the challenges with servers in the System/Application Domain is that the knowledge becomes specialized. People tend to focus on areas of specialty. For example, common security issues with an e-mail server would likely be known only by technicians who regularly work with the e-mail servers.

> **TIP**
> You should lock down a server using the specific security requirements needed by the hosted application. An e-mail server requires one set of protections; a database server requires a different set.

Threats, Vulnerabilities, and Impact

When a threat exploits a vulnerability, it results in a loss. The **impact** identifies the severity of the loss.

A threat is any circumstance or event with the potential to cause a loss. You can also think of a threat as any activity that represents a possible danger. Threats are always present and cannot be eliminated, but they may be controlled.

Threats have independent probabilities of occurring that often are unaffected by an organizational action. As an example, an attacker may be an expert in attacking Web servers hosted on Apache. There is very little a company can do to stop this attacker from trying to attack. However, a company can reduce or eliminate vulnerabilities to reduce the attacker's chance of success.

Threats are attempts to exploit vulnerabilities that result in the loss of **confidentiality**, **integrity**, or **availability** of a business asset. The protection of confidentiality, integrity, and availability is a common security objective for information systems.

Figure 1-2 shows these three security objectives as a protective triangle. If any side of the triangle is breached or fails, security fails. In other words, risks to confidentiality, integrity, or availability represent potential loss to an organization. Because of this, a significant amount of risk management is focused on protecting these resources.

NOTE

Confidentiality, integrity, and availability are often referred to as the *security triad*.

- **Confidentiality**—Preventing unauthorized disclosure of information. Data should be available only to authorized users. Loss of confidentiality occurs when data is accessed by someone who should not have access to it. Data is protected using access controls and encryption technologies.
- **Integrity**—Ensuring data or an IT system is not modified or destroyed. If data is modified or destroyed, it loses its value to the company. Hashing is often used to ensure integrity.
- **Availability**—Ensuring data and services are available when needed. IT systems are commonly protected using fault tolerance and redundancy techniques. Backups are used to ensure the data is retained even if an entire building is destroyed.

TIP

The method used to take advantage of a vulnerability can also be referred to as an *exploit*.

A vulnerability is a weakness. It could be a procedural, technical, or administrative weakness. It could be a weakness in physical security, technical security, or operational security. Just as all threats don't result in a loss, all vulnerabilities don't result in a loss. It's only when an attacker is able to exploit the vulnerability that a loss to an asset occurs.

FIGURE 1-2

Security objectives for information and information systems.

Vulnerabilities may exist because they've never been corrected. They can also exist if security is weakened either intentionally or unintentionally.

Consider a locked door used to protect a server room. A technician could intentionally unlock it to make it easier to access. If the door doesn't shut tight on its own, it could accidentally be left open. Either way, the server room becomes vulnerable.

The impact is the amount of the loss. The loss can be expressed in monetary terms, such as $5,000.

The value of hardware and software is often easy to determine. If a laptop is stolen, you can use the purchase value or the replacement value. However, some losses aren't easy to determine. If that same laptop held data, the value of the data is hard to estimate.

You can use descriptive terms instead of monetary terms to describe the impact. For example, you can describe losses in relative terms, such as high, medium, or low.

An organization quantifies these terms by describing the potential harm. The harm might be to operations, such as the inability to perform critical business functions. It might be to assets, such as hardware or facilities. The harm might be to individuals, such as loss of personal information, injury, or loss of life. It might be to other organizations, resulting in financial losses or damaged relationships. The harm could also be to the nation, affecting government operations or national security.

NIST SP 800-30, published by the National Institute of Standards and Technology, includes the following terms as examples when threats exploit vulnerabilities:

- **Very High**—Indicates multiple severe or catastrophic adverse effects. *Severe* or *catastrophic* indicates a loss of critical business functions. This loss might result in major financial losses or serious injuries to personnel.
- **High**—Indicates a severe or catastrophic adverse effect. Note that *high* indicates one adverse effect. *Very high* indicates multiple adverse effects.
- **Moderate**—Indicates a serious adverse effect. *Serious* indicates critical business functions are significantly degraded. The organization might still be able to operate, but not as effectively as normal. The resulting damage can be significant.
- **Low**—Indicates a limited adverse effect. *Limited* indicates critical business functions are degraded. The resulting damage is minor.
- **Very Low**—Indicates a negligible adverse effect. *Negligible* indicates the impact on critical business functions is small and unnoticeable.

Risk Management and Its Importance to the Organization

Risk management is the practice of identifying, assessing, controlling, and mitigating risks. Threats and vulnerabilities are key drivers of risk. Identifying the threats and vulnerabilities that are relevant to the organization is an important step. You can then take action to reduce potential losses from these risks.

It's important to realize that risk management isn't intended to be risk elimination. That isn't a reasonable goal. Instead, risk management attempts to identify the risks that can be minimized and implements controls to do so. Risk management includes several elements:

- **Assess risks**—Risk management starts with a **risk assessment** or risk analysis. There are multiple steps to a risk assessment:
  - Identify the IT assets of an organization and their value. This can include data, hardware, software, services, and the IT infrastructure.
  - Identify threats and vulnerabilities to these assets. Prioritize the threats and vulnerabilities.
  - Identify the likelihood a vulnerability will be exploited by a threat. These are your risks.
  - Identify the impact of a risk. Risks with higher impacts should be addressed first.
- **Identify risks to manage**—You can choose to avoid, share or transfer, mitigate, or accept risks. The decision is often based on the likelihood of the risk occurring and the impact it will have if it occurs.
- **Select controls**—After you have identified what risks to address, you can identify and select control methods. Control methods are also referred to as countermeasures. Controls are primarily focused on reducing vulnerabilities and impact.
- **Implement and test controls**—Once the controls are implemented, you can test them to ensure they provide the expected protection.
- **Evaluate controls**—Risk management is an ongoing process. You should regularly evaluate implemented controls to determine if they still provide the expected protection. Evaluation is often done by performing regular vulnerability assessments.

How Risk Affects an Organization's Survivability

Profitability and survivability were presented earlier in the chapter. You should also consider them when identifying which risks to manage. Consider both the cost to implement the control and the cost of not implementing the control. As mentioned previously, spending money to manage a risk rarely adds profit. The important point is that spending money on risk management can help ensure a business's survivability.

As an example, consider data and backups. Data is often one of the most valuable assets a business owns. It can include customer data. It can include accounting data such as accounts payable and accounts receivable. It can include employee data. The list goes on and on. This data is integral to the success of a business, so it is often backed up regularly.

Imagine that a business spends $15,000 a year on data backups. This cost will not increase revenue or profits. Imagine that in a full year's time, data is never lost and the backups are never needed. If profitability is the only consideration, management may decide to eliminate this cost. Backups are stopped. The next year, data could be lost, causing the company to fail and go bankrupt.

The cost does need to be considered against profitability, though. For example, if a company earns only $10,000 in profit a year, it doesn't make sense to spend $15,000 a year to protect the data.

On the other hand, imagine a company with $100,000 in annual profits. They choose not to spend the $15,000 on backups. Then a virus spreads through the enterprise, destroying all customer and accounting data. The company no longer has reliable records of accounts receivable. No one has access to the customer base. This can be a business-ending catastrophe.

Reasonableness

A company doesn't need to manage every possible risk. Some risks are reasonable to manage while others are not.

Reasonableness is a test that can be applied to risk management to determine if the risk should be managed. It's derived from the reasonable-person standard in law. In short, you should answer this question. "Would a reasonable person be expected to manage this risk?"

Risks that don't meet the reasonableness test are accepted. For example, the threat of nuclear war exists. A company could spend resources on building bomb shelters for all employees and stocking them with food and water to last 30 years. However, this just isn't reasonable.

As another example, consider a company located on the east coast of Florida. Hurricanes are a very real threat and should be considered. However, the likelihood of a major earthquake hitting the east coast of Florida is relatively minor and doesn't need to be addressed. A business in San Francisco, however, has different concerns. An earthquake there is a real threat, but a hurricane is not. So, for San Francisco, the risk of a hurricane is readily accepted while risk of an earthquake may not be accepted.

Balancing Risk and Cost

The cost to manage the risk must be balanced against the impact value. The costs can be measured in actual monetary values if they are available. You can also balance the costs using relative values such as low, medium, and high.

Table 1-1 shows an example of how the relative values can be assigned. Likelihood values are shown vertically, while impact values are shown horizontally. If a threat has a 0 to 10 percent likelihood of occurring, it is assigned a value of low. If the value is between 11 and 50 percent, the value is medium. If the value is between 51 and 100, the value is high. Similarly, the impact can be ranked as low, medium, and high.

TABLE 1-1 A threat-likelihood-impact matrix.

	LOW IMPACT 10	MEDIUM IMPACT 50	HIGH IMPACT 100
High threat likelihood 100 percent (1.0)	$10 \times 1 = 10$	$50 \times 1 = 50$	$100 \times 1 = 100$
Medium threat likelihood 50 percent (.50)	$10 \times .50 = 5$	$50 \times .50 = 25$	$100 \times .50 = 50$
Low threat likelihood 10 percent (.10)	$10 \times .10 = 1$	$50 \times .10 = 5$	$100 \times .10 = 10$

TIP

You can create a more detailed likelihood-impact matrix. For example, instead of assigning values of low, medium, and high for the threat likelihood, you can assign actual percentages. You can also use more categories instead of just three. This allows greater separation between the categories. Similarly, you can assign any number within a range to the impact. The matrix in the table uses a range of 10, 50, and 100, but you could use any numbers between 1 and 100, if desired.

The potential of some risks to occur is very high and the impact is high, giving you an easy choice. For example, systems without antivirus software will become infected. The threat is common. The likelihood is high. If or when it happens, an infected system can result in the compromise or destruction of all the business's data. The impact is also high. This risk needs to be mitigated. The cost of antivirus software is far less than the impact costs. Therefore, antivirus software is commonly used in business.

Other times, the likelihood is low but the impact is high. For example, the risk of fire in a data center is low. However, the impact is high. A business will often have fire detection and suppression equipment to prevent the impact if a fire occurs. Insurance is also purchased to reduce the impact if a fire does cause damage.

Role-Based Perceptions of Risk

Ideally, all personnel within an organization will readily understand the threat to a company's health if risk is not managed. Unfortunately, risks and risk management are often perceived quite differently.

One of the challenges with effective risk management is achieving a proper balance between security and usability. Consider Figure 1-3. In the diagram on the left, the computers are completely locked down with a high level of security. Users are unable to use them to adequately perform their job. On the right, the computers are easy to use but security is neglected. In the middle, a balance between the two has been achieved.

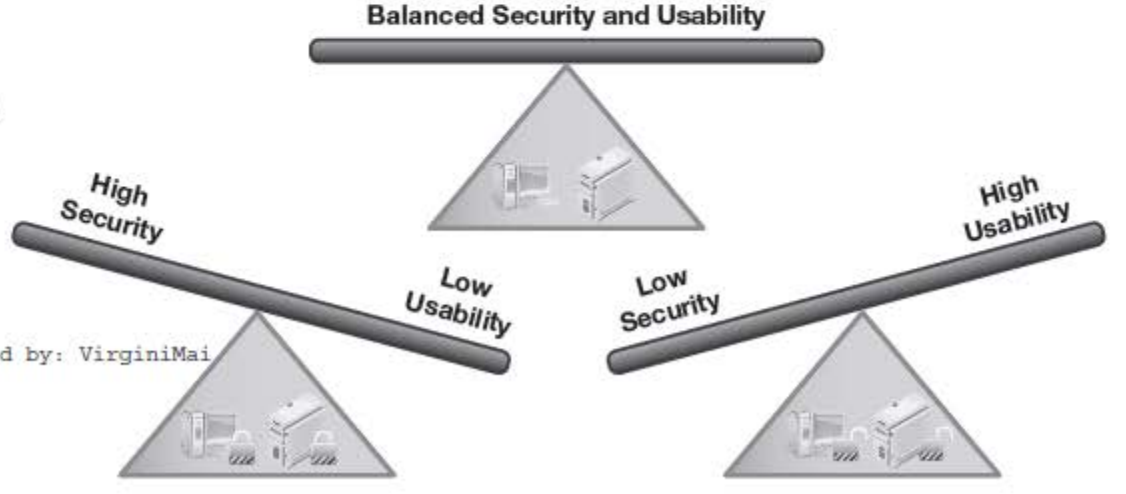


FIGURE 1-3
Balancing security and usability in an organization.

Balanced security rarely satisfies everyone. Security personnel want to lock systems down tighter. End users find the security controls inconvenient and want more usability.

It is common for individuals in the followings roles to have different perceptions of risk:

- **Management**—Management is concerned mostly with profitability and survivability. Since attacks can result in loss of confidentiality, integrity, or availability, management is willing to spend money to mitigate risks. However, their view of the risk is based on the costs of the risk and the costs of the controls. Management needs accurate facts to make decisions on which controls to implement to protect company assets.
- **System administrator**—Administrators are responsible for protecting the IT systems. When they understand the risks, they often want to lock systems down as tight as possible. Administrators are often highly technical individuals. System administrators sometimes lose sight of the need to balance security costs with profitability.
- **Tier 1 administrator**—Tier 1 administrators are the first line of defense for IT support (thus the "tier 1" part of the name). When a user needs assistance, a tier 1 administrator is often called. They may be more concerned with usability than security or profitability. These administrators are given limited administrative permissions. They often view the security controls as hindrances to perform their job and don't always recognize the importance of the controls. For example, the need to use a change management process isn't always understood. A well-meaning technician may bypass a change management process to solve one problem but unintentionally create another problem. These unapproved changes can result in business losses.
- **Developer**—Some companies have in-house application developers. They write applications that can be used in-house or sold. Many developers have adopted a secure computing mindset. They realize that security needs to be included from the design stage all the way to the release stage. When developers haven't adopted a security mindset, they often try to patch security holes at the end of the development cycle. This patching mindset rarely addresses all problems, resulting in the release of vulnerable software.
- **End user**—End users simply want the computer to work for them. They are most concerned with usability. They often don't understand the reason for the security controls and restrictions. Instead, security is viewed as an inconvenience. Well-meaning users often try to circumvent controls so they can accomplish their job. For example, USB thumb drives often transport viruses without the user's knowledge. Companies frequently implement policies restricting the use of thumb drives. When a user needs to transfer a file from one computer to another, the USB thumb drive can be tempting.

TIP

You can restrict the use of thumb drives through a written policy telling people not to use them. You can also use technical controls to prevent use of thumb drives. Computer users can easily ignore a written policy, but they can't easily bypass a technical control. A best practice is to create and enforce both types of policies—written and technical.

You can address the perceptions of these different role holders through targeted training. Some training can include all employees. Other training should be targeted to specific roles. Targeted training helps each role holder better understand the big picture. It can also help them understand the importance of security and its value to the success of the company.

People responsible for managing risks must take all perceptions into account. This is especially true if any of the controls can be bypassed.

For example, theft of laptops is a common problem for some companies. An employee can leave the laptop to take a break at a conference only to come back and find the laptop gone. This risk can almost be eliminated if the company purchases hardware locks. The lock can secure the laptop to a desk or other furniture. However, if users don't perceive the risk as valid, they may simply not use the lock. In addition to purchasing the lock, steps need to be taken to train the users.

Risk Identification Techniques

You learned about risk and losses earlier in this chapter. Risk is the likelihood that a loss will occur. Losses occur when a threat exposes a vulnerability. In order to identify risks, you'll need to take three steps:

- Identify threats.
- Identify vulnerabilities.
- Estimate the likelihood of a threat exploiting a vulnerability.

The following sections explore these concepts.

Identifying Threats

A threat is any circumstance or event with the potential to cause a loss. Said another way, it is any activity that represents a possible danger. The loss or danger is directly related to one of the following:

- **Loss of confidentiality**—Someone sees your password or a company's "secret formula."
- **Loss of integrity**—An e-mail message is modified in transit, a virus infects a file, or someone makes unauthorized changes to a Web site.
- **Loss of availability**—An e-mail server is down and no one has e-mail access, or a file server is down so data files aren't available.

Threat identification is the process of creating a list of threats. This list attempts to identify all the possible threats to an organization. This is no small task. The list can be extensive.

Threats are often considered in the following categories:

- **External or internal**—External threats are outside the boundary of the organization. They can also be thought of as risks that are outside the control of the organization. Internal threats are within the boundary of the organization. They could be related to employees or other personnel who have access to company resources. Internal threats can be related to any hardware or software controlled by the business.
- **Natural or man-made**—Natural threats are often related to weather such as hurricanes, tornadoes, and ice storms. Earthquakes and tsunamis are also natural threats. A human or man-made threat is any threat from a person. Any attempt to sabotage resources is a man-made threat. Fire could be man-made or natural depending on how the fire is started.
- **Intentional or accidental**—Any deliberate attempt to compromise confidentiality, integrity, or availability is intentional. Employee mistakes or user error are accidental threats. A faulty application that corrupts data could be considered accidental.

One method used to identify threats is through a brainstorming session. In a brainstorming session, participants throw out anything that pops into their heads. All ideas are written down without any evaluation. This creative process helps bring up ideas that may be missed when a problem is only analyzed logically.

Some examples of threats to an organization include:

- An unauthorized employee trying to access data
- Any type of malware
- An attacker defacing a Web site
- Any DoS or DDoS attack
- An external attacker trying to access data
- Any loss of data
- Any loss of services
- A social engineer tricking an employee into revealing a secret
- Earthquakes, floods, or hurricanes
- A lightning strike
- Electrical, heating, or air conditioning outages
- Fires

> **TIP**
> A denial of service (DoS) attack is an attack that attempts to disrupt a service. A DoS attack results in the service being unavailable. A distributed denial of service (DDoS) attack originates from multiple attackers.

All these threats represent possible risks if they expose vulnerabilities.

Of course, you will identify different threats and vulnerabilities depending on the organization. Every organization has threats and vulnerabilities specific to it. In fact, a business with multiple locations may have some threats and vulnerabilities unique to one location.

Identifying Vulnerabilities

You learned earlier that a vulnerability is a weakness. Vulnerabilities are apparent when threats exploit them. Ideally, you'll identify the weaknesses before threats exploit them. Luckily, most organizations have a lot of sources that can help you.

Some of the sources you can use are:

- **Audits**—Many organizations are regularly audited. Systems and processes are checked to verify a company complies with existing rules and laws. Auditors document their findings in reports. These reports list findings that directly relate to weaknesses.
- **Certification and accreditation records**—Several standards exist to examine and certify IT systems. If the system meets the standards, the IT system can be accredited. The entire process includes detailed documentation. This documentation can be reviewed to identify existing and potential weaknesses.
- **System logs**—Many types of logs can be used to identify threats. Audit logs can determine if users are accessing sensitive data. Firewall logs can identify traffic that is trying to breach the network. Firewall logs can also identify computers taken over by malware and acting as zombies. DNS logs can identify unauthorized transfer of data.
- **Prior events**—Previous security incidents are excellent sources of data. As evidence of risks that already occurred, they help justify controls. They show the problems that have occurred and can show trends. Ideally, weaknesses from a security incident will be resolved right after the incident. In practice, employees are sometimes eager to put the incident behind them and forget it as soon as possible. Even if documentation doesn't exist on the incident, a few key questions can uncover the details.
- **Trouble reports**—Most companies use databases to document trouble calls. These databases can contain a wealth of information. With a little bit of analysis, you can use them to identify trends and weaknesses.
- **Incident response teams**—Some companies have incident response teams. These teams will investigate all the security incidents within the company. You can interview team members and get a wealth of information. These teams are often eager to help reduce risks.

TIP

Some malware can take control of multiple computers and control them as robots. The controlling computer issues attack commands and the computers attack. The individual computers are referred to as *zombies*. The network of controlled computers is called a *botnet*.

Using the Seven Domains of a Typical IT Infrastructure to Identify Weaknesses

Another way of identifying weaknesses is by examining the seven domains of a typical IT infrastructure. These domains were presented earlier in this chapter. Each domain can be examined individually. Further, each domain can be examined by experts in that domain. The following list gives you some examples in each of these domains:

- **User Domain**—Social engineering represents a big vulnerability. Sally gets a call. "Hi. This is Bob from the help desk. We've identified a virus on your computer." Bob then attempts to walk Sally though a long detailed process and then says "Why don't I just fix this for you? You can get back to work. All I need is your password."

- **Workstation Domain**—Computers that aren't patched can be exploited. If they don't have antivirus software, they can become infected.
- **LAN Domain**—Any data on the network that is not secured with appropriate access controls is vulnerable. Weak passwords can be cracked. Permissions that aren't assigned properly allow unauthorized access.
- **LAN-to-WAN Domain**—If users are allowed to visit malicious Web sites, they can mistakenly download malicious software. Firewalls with unnecessary ports open allow access to the internal network from the Internet.
- **WAN Domain**—Any public-facing server is susceptible to DoS and DDoS attacks. A File Transfer Protocol (FTP) server that allows anonymous uploads can host warez from black-hat hackers.
- **Remote Access Domain**—Remote users may be infected with a virus but not know it. When they connect to the internal network via remote access, the virus can infect the network.
- **System/Application Domain**—Database servers can be subject to SQL injection attacks. In a SQL injection attack, the attacker can read the entire database. SQL injection attacks can also modify data in the database.

TIP

Warez (pronounced as "wares") is a term that describes pirated files. Examples include pirated games, MP3 files, and movies. A warez site often includes hacking tools, which anyone can download, including hackers.

TIP

A *SQL injection attack* tries to access data from Web sites. SQL statements are entered into text boxes. If the Web site isn't programmed defensively, these SQL statements can be executed against a database. Some programs are available that can launch a SQL injection attack and retrieve an entire database.

This list certainly isn't complete. The number of vulnerabilities discovered in IT systems is constantly growing. The MITRE Corporation catalog **Common Vulnerabilities and Exposures (CVE)** includes more than 40,000 items.

Using Reason When Identifying Vulnerabilities

Reasonableness was covered earlier in this chapter. As a reminder, reasonableness answers the question, "Would a reasonable person be expected to manage this risk?" In this context, you can think of it as, "Would a reasonable person be expected to reduce this vulnerability?"

You should focus on vulnerabilities within the organization or within the system being evaluated. External vulnerabilities are often not addressed. For example, a server will likely fail if air conditioning fails. You would address this when identifying vulnerabilities for a server room. You wouldn't address it for each of the 50 servers in the server room. Similarly, the commercial power may fail. You may address this by having uninterruptible power supplies (UPSs) and generators. However, you don't need to identify alternatives for the commercial power company.

Pairing Threats with Vulnerabilities

The third step when identifying risks is to pair the threats with vulnerabilities. Threats are matched to existing vulnerabilities to determine the likelihood of a risk.

TABLE 1-2 Risk and trust levels of common network zones.

THREAT	VULNERABILITY	IMPACT
An unauthorized employee tries to access data hosted on a server.	The organization doesn't use adequate authentication and access controls.	The possible loss would depend on the sensitivity of the data and how it's used. For example, if the unauthorized employee accessed salary data and freely shared it, this could impact morale and productivity.
Any type of malware, such as viruses or worms, enters the network.	Antivirus software doesn't detect the virus.	The virus could be installed on systems. Viruses typically result in loss of confidentiality, integrity, or availability.
An attacker modifies or defaces a Web site.	The Web site isn't protected.	Depending on how the attacker modifies the Web site, the credibility of the company could be affected.
A social engineer tricks an employee into revealing a password.	Users aren't adequately trained.	Passwords could be revealed. An attacker who obtains a password could take control of the user's account.

The "Identifying Threats" section listed several threats. Table 1-2 takes a few of those threats and matches them to vulnerabilities to identify possible losses.

The following formula is often used when pairing threats with vulnerabilities:

Risk = Threat × Vulnerability

However, this isn't a true mathematical formula. Threat and vulnerability don't always have numerical values. Instead, the formula shows the relationship between the two.

If you can identify the value of the asset, the formula is slightly modified to:

Total Risk = Threat × Vulnerability × Asset Value

Risk Management Techniques

After identifying risks, you need to decide what you want to do about them. Risk management can be thought of as handling risk. It's important to realize that risk management is not risk elimination. A business that is unwilling to take any risks doesn't stay in business long. The cost to eliminate all risks will consume all the profits.

The ultimate goal of risk management is to protect the organization. It helps ensure a business can continue to operate and earn a profit. Risk management includes several steps. They include:

- Identifying risks
- Assessing risks
- Determining which risks will be handled and which risks will be accepted
- Taking steps to reduce risk to an acceptable level

When deciding how to handle a risk, you can choose to avoid, share or transfer, mitigate, or accept the risk. These techniques are explained in the following sections.

Avoidance

One of the ways you manage risk is by simply avoiding it. The primary reason to **avoid** a risk is that the impact of the risk outweighs the benefit of the asset.

An organization can avoid risk by:

- **Eliminating the source of the risk**—The company can stop the risky activity. For example, a company may have a wireless network that is vulnerable to attacks. The risk could be avoided by removing the wireless network. This can be done if the wireless network isn't an important asset in the company.
- **Eliminating the exposure of assets to the risk**—The company can move the asset. For example, a data center could be at risk because it is located where earthquakes are common. It could be moved to an earthquake-free zone to eliminate this risk. The cost to move the data center will be high. However, if the risk is unacceptable and the value of the data center is high, it makes sense.

Share or Transfer

You can share or **transfer** risk by shifting responsibility to another party. Risk transfer shifts the entire responsibility or liability. Risk sharing shifts a portion of the responsibility or liability. Organizations can outsource part or all of the activity.

- **Insurance**—You purchase insurance to protect your company from a loss. If a loss occurs, the insurance covers it. Many types of insurance are available, including fire insurance.
- **Outsourcing the activity**—For example, your company may want to host a Web site on the Internet. The company can host the Web site with a Web hosting provider. Your company and the provider can agree on who assumes responsibility for security, backups, and availability.

Mitigation

You reduce risk by reducing vulnerabilities, and the primary strategy in this process is to **mitigate** risk. Risk mitigation is also known as *risk reduction*.

You reduce vulnerabilities by implementing controls or countermeasures. The cost of a control should not exceed the benefit. Determining costs and benefits often requires a cost-benefit analysis, which is covered later in this chapter.

Some examples of mitigation steps are:

- **Alter the physical environment**—Replace hubs with switches. Locate servers in locked server rooms.
- **Change procedures**—Implement a backup plan. Store a copy of backups offsite, and test the backups.
- **Add fault tolerance**—Use Redundant Array of Independent Disks (RAID) for important data stored on disks. Use failover clusters to protect servers.
- **Modify the technical environment**—Increase security on the firewalls. Add intrusion detection systems. Keep antivirus software up to date.
- **Train employees**—Train technical personnel on how to implement controls. Train end users on social engineering tactics.

TIP

Controls are often referred to as either preventive or detective. *Preventive controls* attempt to deter or prevent the risk from occurring. Examples include increasing physical security and training personnel. *Detective controls* try to detect activity that may result in a loss. Examples include antivirus software and intrusion detection systems.

Often the goal is not to eliminate the risk but, instead, to make it too expensive for the attacker. Consider the following two formulas:

- **Attacker's Cost < Attacker's Gain**—When this is true, it is appealing to the attacker.
- **Attacker's Cost > Attacker's Gain**—When this is true, the attacker is less likely to pursue the attack.

Cryptography is one of the ways to increase the attacker's cost. If your company sends data across the network in cleartext, it can be captured and analyzed. If the company encrypts the data, an attacker must decrypt it before analyzing it. The goal of the encryption isn't to make it impossible to decrypt the data. Instead, the goal is to make it too expensive or too time-consuming for the attacker to crack it.

Acceptance

You can also choose to **accept** a risk. A company can evaluate a risk, understand the potential loss, and choose to accept it. This is commonly done when the cost of the control outweighs the potential loss.

For example, consider the following scenario: A company hosts a Web server used for e-commerce. The Web server generates about $1,000 per month in revenue. The server could be protected using a failover cluster. However, estimates indicate that a failover cluster will cost approximately $10,000. If the server goes down, it may be down for only one or two hours, which equates to less than $3. (Revenue per hour = $1,000 × 12 / 365 / 24 = $1.37.)

NOTE

A simple failover cluster could include two servers. One server provides the service to users and the other server acts as a spare. If the online server fails, the spare server can sense the failure and automatically take over.

The decision to accept a loss becomes easier if you have evaluated the costs against the benefits, which is known as a **cost-benefit analysis (CBA)**. A cost-benefit analysis is useful when choosing any of the techniques to manage risk.

Cost-Benefit Analysis

You perform a cost-benefit analysis to help determine which controls or countermeasures to implement. If the benefits outweigh the costs, the control is often selected.

A CBA compares the business impact with the cost to implement a control. For example, the loss of data on a file server may represent the loss of $1 million worth of research. Implementing a backup plan to ensure the availability of the data may cost $10,000. In other words, you would spend $10,000 to save $1 million. This makes sense.

A CBA starts by gathering data to identify the costs of the controls and benefits gained if they are implemented.

- **Cost of the control**—This includes the purchase costs plus the operational costs over the lifetime of the control.
- **Projected benefits**—This includes the potential benefits gained from implementing the control. You identify these benefits by examining the costs of the loss and how much the loss will be reduced if the control is implemented.

A control doesn't always eliminate the loss. Instead, the control reduces it. For example, annual losses for a current risk may average $100,000. If a control is implemented, these losses may be reduced to $10,000. The benefit of the control is $90,000.

You can use the following formula to determine if the control should be used:

Loss before Control − Loss after Control = Cost of Control

Imagine the company lost $100,000 last year without any controls implemented. You estimate you'll lose $12,000 a year if the control is implemented. The cost of the control is estimated at $7,000. The formula is:

$100,000 − $7,000 (Cost of Control) − $12,000 (Expected Residual Loss) = $81,000

This represents a benefit of $81,000.

One of the biggest challenges when performing a CBA is getting accurate data. While current losses are often easily available, future costs and benefits need to be estimated. Costs are often underestimated. Benefits are often overestimated.

The immediate costs of a control are often available. However, the ongoing costs are sometimes hidden. Some of the hidden costs may be:

- Costs to train employees
- Costs for ongoing maintenance
- Software and hardware renewal costs

If the costs outweigh the benefits, the organization might choose not to implement the control. Instead, it might choose to accept, share or transfer, or avoid the risk.

Residual Risk

Residual risk is the risk that remains after you apply controls. It's not feasible to eliminate all risks. Instead, you take steps to reduce the risk to an acceptable level. The risk that's left is residual risk.

Earlier in this chapter, the following two formulas were given for risk:

Risk = Threat × Vulnerability

Total Risk =Threat × Vulnerability × Asset Value

You can calculate residual risk with the following formula:

Residual Risk =Total Risk − Controls

Senior management is responsible for any losses due to residual risk. They decide whether a risk should be avoided, shared or transferred, mitigated, or accepted. They also decide what controls to implement. Any resulting loss due to their decisions falls on their shoulders.

CHAPTER SUMMARY

Risks occur when threats exploit vulnerabilities, resulting in a loss. The loss can compromise business functions and business assets. Losses also drive business costs. Risk management helps a company identify risks that need to be reduced. The first steps in risk management are to identify threats and vulnerabilities. These can then be paired to help determine the severity of the risk.

You can manage risks by choosing one of four techniques: A risk can be avoided, shared or transferred, mitigated, or accepted. The primary risk management technique is risk mitigation. Risk mitigation is also known as risk reduction or risk treatment. You reduce vulnerabilities by implementing controls.

KEY CONCEPTS AND TERMS

Accept
Availability
Avoid
Common Vulnerabilities and Exposures (CVE)
Confidentiality
Controls
Cost-benefit analysis (CBA)
Impact
Intangible value
Integrity
Mitigate
Profitability
Reasonableness
Residual risk
Risk
Risk assessment
Risk management
Survivability
Tangible value
Threat
Total risk
Transfer
Vulnerability

CHAPTER 1 ASSESSMENT

1. Which one of the following properly defines risk?
   A. Threat × Mitigation
   B. Vulnerability × Controls
   C. Controls − Residual Risk
   D. Threat × Vulnerability

2. Which one of the following properly defines total risk?
   A. Threat − Mitigation
   B. Threat × Vulnerability × Asset Value
   C. Vulnerability − Controls
   D. Vulnerability × Controls

3. You can completely eliminate risk in an IT environment.
   A. True
   B. False

4. Which of the following are accurate pairings of threat categories? (Select two.)
   A. External and internal
   B. Natural and supernatural
   C. Intentional and accidental
   D. Computer and user

5. A loss of client confidence or public trust is an example of a loss of _____.

6. A _____ is used to reduce a vulnerability.

7. As long as a company is profitable, it does not need to consider survivability.
   A. True
   B. False

8. What is the primary goal of an information security program?
   A. To eliminate losses related to employee actions
   B. To eliminate losses related to risk
   C. To reduce losses related to residual risk
   D. To reduce losses related to loss of confidentiality, integrity, and availability

9. The _____ is an industry-recognized standard list of common vulnerabilities.

10. Which of the following is a goal of risk management?
    A. To identify the correct cost balance between risk and controls
    B. To eliminate risk by implementing controls
    C. To eliminate the loss associated with risk
    D. To calculate value associated with residual risk

11. If the benefits outweigh the cost, a control is implemented. Costs and benefits are identified by completing a _____.

12. A company decides to reduce losses of a threat by purchasing insurance. This is known as risk _____.

13. What can you do to manage risk? (Select three.)
    A. Accept
    B. Transfer
    C. Avoid
    D. Migrate

14. You have applied controls to minimize risk in the environment. What is the remaining risk called?
    A. Remaining risk
    B. Mitigated risk
    C. Managed risk
    D. Residual risk

15. Who is ultimately responsible for losses resulting from residual risk?
    A. End users
    B. Technical staff
    C. Senior management
    D. Security personnel

Managing Risk: Threats, Vulnerabilities, and Exploits

CHAPTER 2

A KEY STEP WHEN MANAGING RISKS is to first understand and manage the source. This includes threats and vulnerabilities, and especially threat/vulnerability pairs. Once you understand these elements, it's much easier to identify mitigation techniques. Exploits are a special type of threat/vulnerability pair that often includes buffer overflow attacks.

Fortunately, the U.S. federal government has initiated several steps to help protect information technology (IT) resources. The National Institute of Standards and Technology has done a lot of research on risk management. The results of this research are freely available in the form of Special Publications. Additionally, the Department of Homeland Security oversees several other initiatives related to IT security.

Chapter 2 Topics

This chapter covers the following topics and concepts:

- What threats are and how they can be managed
- What vulnerabilities are and how they can be managed
- What exploits are and how they can be managed
- Which risk management initiatives the U.S. federal government sponsors

Chapter 2 Goals

When you complete this chapter, you will be able to:

- Describe the uncontrollable nature of threats
- List unintentional and intentional threats
- Identify best practices for managing threats

- Identify threat/vulnerability pairs
- Define mitigation
- List and describe methods used to mitigate vulnerabilities
- Identify best practices for managing vulnerabilities
- Define exploit
- Describe the perpetrator's role in vulnerabilities and exploits
- Identify mitigation techniques
- Identify best practices for managing exploits
- Identify the purpose of different U.S. federal government risk management initiatives

Understanding and Managing Threats

A *threat* is any activity that represents a possible danger. This includes any circumstances or events with the potential to adversely impact confidentiality, integrity, or availability of a business's assets.

Threats are a part of the equation that creates risk:

Risk = Vulnerability × Threat

Any attempt to manage risk requires a thorough knowledge of threats. This section includes the following topics:

- The uncontrollable nature of threats
- Unintentional threats
- Intentional threats
- Best practices for managing threats within your IT infrastructure

The Uncontrollable Nature of Threats

It's important to realize a few basic facts about threats. These include:

- Threats can't be eliminated.
- Threats are always present.
- You can take action to reduce the potential for a threat to occur.
- You can take action to reduce the impact of a threat.
- You cannot affect the threat itself.

Consider the threat of a car thief. Car thieves steal cars, and you can't prevent that. However, you can take steps to either enhance or reduce the threat against your car. To increase the chances of a thief stealing your car, you can park it in a busy parking lot. Leave the keys in and the car running. Leave a $20 bill on the dashboard. Leave a few expensive items on the front seat. It's just a matter of time before your car is stolen.

However, you can take different steps to reduce the potential threat and impact. Remove the keys and lock the doors. Install a car alarm. Hide valuables in the trunk. A car thief might still visit that parking lot, but it is less likely that your car will be stolen.

Sometimes a car thief looks for a specific model, year, and color of car. If your car is a match, the thief will likely steal it no matter what you do. However, you can reduce the impact of the loss. If you have insurance, it will reimburse you if your car is never recovered.

Threats to IT are similar. Lightning strikes hit buildings. Malware authors constantly write new programs. Script kiddies run malware programs just to see what they can do. Professional attackers spend 100 percent of their work time trying to break into government and corporate networks. You can't stop them.

However, there are many things you can do to reduce the potential harm that these threats can do to your network. You can take steps to reduce the impact of these threats.

Unintentional Threats

Unintentional threats are threats that don't have a perpetrator. They don't occur because someone is specifically trying to attack. Natural events and disasters, human errors, and simple accidents are all considered unintentional.

There are four primary categories of unintentional threats. They are:

- **Environmental**—Threats affecting the environment. This includes weather events such as floods, tornadoes, and hurricanes. Earthquakes and volcanoes are environmental threats too. Illnesses or an epidemic can cause a loss to the labor force and reduce the availability of systems.
- **Human**—Errors caused by people. A simple keystroke error can cause incorrect or invalid data to be entered. A user may forget to enter key data. A technician could fail to follow a backup procedure resulting in an incomplete backup. An administrator may write incomplete or incorrect backup procedures. Undiscovered software bugs can also cause serious problems.
- **Accidents**—Anything from a minor mishap to a major catastrophe. A backhoe digging a new trench for new cables can accidentally cut power or data cables. An employee might accidentally start a fire in a break room.
- **Failures**—Equipment problems. A hard drive can crash. A server can fail. A router can stop routing traffic. The air conditioner might stop blowing cool air, causing multiple systems to overheat and fail. Any of these failures can result in the loss of availability of data or services.

> **TIP**
> You can use a hot, warm, or cold site to provide an alternate location for IT functions.

Although these threats are unintentional, you can address them with a risk management plan. Here are some common methods:

- **Managing environmental threats**—You can purchase insurance to reduce the impact of many environmental threats. A business may decide to move to reduce the threat. For example, a business in the area of the Mount St. Helens volcano can relocate to avoid eruptions. Companies in a hurricane zone can transfer operations elsewhere.
- **Reducing human errors**—Automation and input validation are common methods used to reduce errors. Any process that can be automated will consistently run the same way. Input validation checks data to ensure it is valid before it is used. For example, if a program expects a first name, the input validator checks whether the data looks like a valid name. Rules for a valid first name may be no more than 20 characters, no numbers, and only specific special characters. Input validation can't check to ensure that data is accurate, but it can ensure that data is valid.
- **Preventing accidents**—Contact the 1-800-MISS-DIG company in Michigan, or similar companies or agencies in other states, to identify underground cables before digging. You can stress safety to prevent common accidents.
- **Avoiding failures**—Use fault-tolerant and redundant systems to protect against the immediate impact of failures. A RAID system can help ensure data availability, and failover clusters ensure users can access servers at all times.

Intentional Threats

Intentional threats are acts that are hostile to the organization. One or more perpetrators are involved in carrying out the threat. Perpetrators are generally motivated by one of the following:

- **Greed**—Many attackers want to make money through the attacks. Attackers steal data and use it to perform acts of fraud. They steal customer data from databases and commit identity theft. Criminals steal proprietary data from competitors. Social engineers try to trick users into giving up passwords for financial sites.
- **Anger**—When anger is the motivator, the attacker often wants the victim to pay a price. Anger can result in attempts to destroy assets or disrupt operations. These threats often result in a loss of availability.
- **Desire to damage**—Some attackers just want to cause damage. The result is the same as if an attacker is motivated by anger. It can result in a loss of availability.

Although the preceding list helps you understand what motivates attackers, the items don't identify who the attackers are. Some people still have the image of a bored teenager launching random threats from his or her room. However, attackers are much more sophisticated today.

Some of the more common attackers today are:

- **Criminals**—Opportunities to make money from online attacks have resulted in a growth in criminal activity. Furthermore, criminal activity is far more organized today. This activity includes fraud and theft. For example, *rogueware* tricks users into installing bogus antivirus software. Then they must pay to get it removed. Criminals have extorted millions of dollars using rogueware. More recently, this has morphed into *ransomware*. Criminals restrict access to the system and display messages to the user demanding ransoms to get access to his or her computer and/or files.
- **Advanced persistent threats (APTs)**—Attackers focus on a specific target. APTs have high levels of expertise and almost unlimited resources. Nation states or terrorist groups often sponsor them. They attack both government and private targets. Operation Aurora is an example of an APT attack. Investigations indicate the APT attack originated from China. It attacked several private companies such as Google. A McAfee white paper titled "Revealed: Operation Shady RAT" discusses 71 different APT attacks. Twenty-one of these were government targets. Fifty were private companies.
- **Vandals**—Some attackers are intent on doing damage. They damage just for the sake of damaging something. Their targets are often targets of opportunity.
- **Saboteurs**—A saboteur commits sabotage. This could be sabotage against a competing company or against another country. The primary goal is to cause a loss of availability.
- **Disgruntled employees**—Dissatisfied employees often present significant threats to a company. There are countless reasons why an employee may be dissatisfied; for example, an employee who did not receive a pay raise might be disgruntled. Employees with a lot of access can cause a lot of damage.
- **Activists**—Occasionally, activists present a threat to a company. Activists often operate with a mindset of "the end justifies the means." In other words, if your company does something the activist doesn't approve of, the activist considers it acceptable to attack.
- **Other nations**—International espionage is a constant threat. For example, McAfee's "Operation Shady RAT" white paper details espionage activities widely believed to come from China. Attackers use remote access tools (RATs) to collect information. They have infiltrated several governments and private companies. Many countries include cyberwarfare as a part of their offensive and defensive strategies.
- **Hackers**—Hackers attempt to breach systems. Depending on the goal of the hacker, the motivation may range from innocent curiosity to malicious intent.

TIP

There is a technical difference between a hacker and a cracker. *Hackers* have historically been known as "white-hat hackers" or "ethical hackers"—the good guys. They hack into systems to learn how it can be done, but not for personal gain. *Crackers* have been known as "black-hat hackers" or "malicious hackers"—the bad guys. They hack into systems to damage, steal, or commit fraud. Many black-hat hackers present themselves as white-hat hackers claiming that their actions are innocent. However, most mainstream media put all hackers in the same black-hat category. The general perception is that all hackers are bad guys.

Best Practices for Managing Threats Within Your IT Infrastructure

There are many steps you can take to manage threats within your IT infrastructure. The following list represents steps that IT security professionals consider best practices:

> **TIP**
>
> A security policy may include several individual policies. For example, it could include a password policy, an acceptable use policy, and a firewall policy.

- **Create a security policy**—Senior management identifies and supports the role of security and creates a **security policy**. This policy provides a high-level overview of the goals of security but not details of how to implement security techniques. Managers use this policy to identify resources and create plans to implement the policy. Security policies are an important first step in reducing the impact from threats. Once the security policy is approved, it needs to be implemented and enforced.
- **Purchase insurance**—Purchase insurance to reduce the impact of threats. Companies commonly purchase insurance for fire, theft, and losses due to environmental events.
- **Use access controls**—Require users to authenticate. Grant users access only to what they need. This includes the following two principles:
  - **Principle of least privilege**—Grant users only the rights and permissions they need to perform their job and no more. This prevents users from accidentally or intentionally causing problems.
  - **Principle of need to know**—Grant users access only to the data they need to perform their job and no more. For example, a person may have a security clearance for Secret data. However, that person doesn't automatically receive access to all Secret data. Instead, the person is granted access only to what he or she needs for the job. This helps prevent unauthorized access.

> **NOTE**
>
> Privileges include *rights* and *permissions*. Rights refer to actions users can perform on objects. For example, a user might have the right to change the system time. Permissions refer to object access. For example, a user might have permission to read and modify a file. The *principle of least privilege* includes both rights and permissions. The *principle of need to know* focuses on data permissions.

- **Use automation**—Automate processes as much as possible to reduce human errors.
- **Include input validation**—Test data to determine if it is valid before any applications use it.
- **Provide training**—Use training to increase safety awareness and reduce accidents. You can also use training to increase security awareness to reduce security incidents.
- **Use antivirus software**—Make sure you install antivirus software on all systems. Schedule virus definition updates to occur automatically.
- **Protect the boundary**—Protect the boundary between the intranet and the Internet with a firewall, at a minimum. You can also use intrusion detection systems for an added layer of protection.

CSI Computer Crime and Security Survey 2010/2011

The Computer Security Institute (CSI) completes regular surveys that identify many of the trends related to IT security. The 2010/2011 report includes responses from 5,412 security practitioners.

Some of the notable findings in this report were:

- Malware infections are the most commonly seen attack. Over 67 percent of respondents reported malware infections. This is an increase of 3 percent from the previous year. The lowest was 50 percent in 2007.
- About 29 percent reported zombies within their network. A zombie is a computer joined to a botnet. This is an increase of 5 percent from the previous year.
- Most respondents attribute losses to outsiders. Almost 60 percent indicated they did not believe any of their losses were due to malicious insiders.
- Only about 25 percent reported insider abuse of network access or e-mail usage. This is a significant reduction from a high of 59 percent in 2007.
- Of respondents reporting incidents, 45.6 percent reported they were the subject of at least one targeted attack. The trend is more attacks from advanced persistent threats (APTs).
- Losses due to financial fraud declined from almost 19 percent to about 8 percent during the period.
- Respondents indicated that regulatory compliance efforts had a positive effect on their security programs.
- Almost half of the organizations reported they were using cloud computing, but only 10 percent indicated they were using cloud-specific security tools.

Understanding and Managing Vulnerabilities

A *vulnerability* can be a weakness in an asset or the environment. You can also consider a weakness as a flaw in any system or any business process.

A vulnerability leads to a risk, but by itself it does not become a loss. The loss occurs when a threat exploits the vulnerability. This is also referred to as a threat/vulnerability pair.

Figure 2-1 shows the flow of a threat to a loss. You can use mitigation techniques to reduce the vulnerability, the loss, or both.

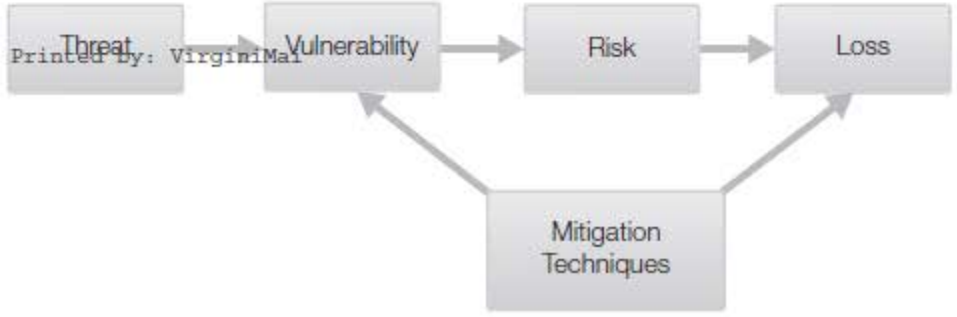


FIGURE 2-1
The flow of threat/vulnerability pairs.

This section presents the following topics:

- Threat/vulnerability pairs
- Vulnerabilities can be mitigated
- Mitigation techniques
- Best practices for managing vulnerabilities within your IT infrastructure

Threat/Vulnerability Pairs

A **threat/vulnerability pair** occurs when a threat exploits a vulnerability. The vulnerabilities provide a path for the threat that results in a harmful event or a loss. It's important to know that both the threat and the vulnerability must come together to result in a loss.

Vulnerabilities depend on your organization. For example, if you're hosting public-facing servers, the servers have several potential weaknesses. However, if you don't have any public-facing servers, there aren't any vulnerabilities for the organization in this area. Thus, the risk is zero.

Table 2-1 shows some examples of threat/vulnerability pairs and the potential losses. This table only scratches the surface. The list of vulnerabilities for any single network can be quite extensive.

TABLE 2-1 Examples of threat/vulnerability pairs and potential losses.

THREAT	VULNERABILITY	HARMFUL EVENT OR LOSS
Fire	Lack of fire detection and suppression equipment	Can be total loss of business
Hurricane, earthquake, tornado	Location	Can be total loss of business
Malware	Lack of antivirus software Outdated definitions	Infection (impact of loss determined by payload of malware)
Equipment failure	Data not backed up	Loss of data availability (impact of loss determined by value of data)
Stolen data	Access controls not properly implemented	Loss of confidentiality of data
Denial of service (DoS) or distributed denial of service (DDoS) attack	Public-facing servers not protected with firewalls and intrusion detection systems	Loss of service availability
Users	Lack of access controls	Loss of confidentiality
Social engineer	Lack of security awareness	Loss depends on the goals and success of attacker

Vulnerabilities Can Be Mitigated

You can mitigate or reduce vulnerabilities, which reduces potential risk. The risk reduction comes from one of the following:

- Reducing the rate of occurrence
- Reducing the impact of the loss

It's rare that a threat is completely eliminated. Instead, it's more common that the risk is reduced to an acceptable level. The remaining risk is referred to as the *residual risk*. Table 2-2 matches the threat/vulnerabilities pairs from Table 2-1 with possible mitigation steps.

TABLE 2-2 Common threat/vulnerability pairs and possible mitigation steps.

THREAT	VULNERABILITY	MITIGATION
Fire	Lack of fire detection and suppression equipment	Install fire detection and suppression equipment Purchase insurance
Hurricane, earthquake, tornado	Location	Purchase insurance Designate alternate sites
Malware	Lack of antivirus software Outdated definitions	Install antivirus software Update definitions at least weekly
Equipment failure	Data not backed up	Back up data regularly Keep copies of backup off-site
Stolen data	Access controls not properly implemented	Implement both authentication and access controls Use principle of "need to know"
DoS or DDoS attack	Public-facing servers not protected with firewalls and intrusion detection systems	Implement firewalls Implement intrusion detection systems
Users	Lack of access controls	Implement both authentication and access controls
Social engineer	Lack of security awareness	Provide training Raise awareness through posters, occasional e-mails, and mini-presentations

Mitigation Techniques

You can use a wide variety of mitigation techniques in any enterprise. As you explore the techniques in this section, keep the following elements in mind:

- The value of the technique
- The initial cost of the technique
- Ongoing costs

For example, antivirus software has an initial cost. This initial cost includes a subscription for updates for a period of time, such as a year. When the subscription expires, it must be renewed.

When estimating the value and cost of any of these techniques, you can consider the value of the resource and the impact of the loss. For example, training in basic social engineering tactics may cost $10,000 a year. However, if users don't receive the training, the company may lose $100,000. This indicates the value of the training is $90,000.

However, there are other variables to consider when estimating the value of a mitigation technique. A company may have lost $100,000 last year. If people are trained, the company estimates it will only lose $5,000 this year. This would give a value of $85,000 to the training. This is calculated as:

Last Year's Loss − Training Cost − This Year's Loss, or
$100,000 − $10,000 − $5,000 = $85,000.

The following list identifies many common mitigation techniques you can use in any enterprise:

- **Policies and procedures**—Written policies and procedures provide standards. These standards make it clear what should be implemented and how. Many organizations start by creating a security policy as mentioned earlier. You should review policies and procedures on a regular basis.
- **Documentation**—Documentation is useful in a wide number of areas. Up-to-date documentation of networks makes problems easier to troubleshoot. Once problems occur, you can repair them more quickly. This results in improved availability times. As the network and systems change, you need to be sure to update documentation.
- **Training**—Training helps employees understand that security is everyone's responsibility. Some training is geared to all users; other training must be targeted to specific users. For example, you should train all end users about social engineers. Train administrators on current threats and vulnerabilities. Train management on risk management strategies. Training is an ongoing event—as things change, you should offer updated training classes.

- **Separation of duties**—The **separation of duties** principle ensures that any single person does not control all the functions of a critical process. It's designed to prevent fraud, theft, and errors. For example, accounting separates accounts receivable from accounts payable. One division accepts and approves bills. The other division pays the approved bills. Separation of duties also helps prevent conflicts of interest.

- **Configuration management**—When system configuration is standardized, systems are easier to troubleshoot and maintain. One method of **configuration management** is to use baselines. For example, you configure a system and then create a system image. You can deploy the image to 100 other systems, so every system is identical. Maintenance of each of these systems is the same. When technicians learn one system, they learn them all. Without a baseline, the systems may be configured 100 different ways. Technicians need to learn how each system is configured before they can provide effective support. Images are updated as the configuration changes.

  Configuration management also ensures that systems are not improperly modified. Most organizations have change management processes in place. This ensures that only authorized changes are made. Compliance auditing is done to ensure that unauthorized changes don't occur.

> **NOTE**
>
> Symantec's Ghost is a common tool used to deploy multiple clients. Ghost allows you to capture images and store them on a DVD or on a Ghost casting server. You can then deploy the image to any client from the DVD. You can also cast the image to multiple clients simultaneously from the server.

- **Version control**—When multiple people work on the same document or the same application, data can be lost or corrupted. **Version control** systems are commonly used with the development of applications. They track all changes and can reduce wasted time and effort, especially if changes need to be reversed. The process requires programmers to check out modules or files before modifying them. After the file is modified, it can be checked in and someone else can modify the file. Some version control software allows multiple changes to be merged into a single file.
- **Patch management**—Over time, you may discover bugs in software. Software bugs are vulnerabilities that can be exploited. When the bugs are discovered, they are patched by vendors; however, attackers also find out about the bugs. Systems that aren't patched are vulnerable to attack. A comprehensive **patch management** policy governs how patches are understood, tested, and rolled out to systems and clients. It should include compliance audits to verify that clients are current. Patch management can also include the ability to quarantine unpatched clients. Patch management is an almost continuous process.

> **NOTE**
>
> Microsoft releases patches on the second Tuesday of every month. This has become known as **Patch Tuesday**. When the patches aren't deployed, attackers can exploit the bugs.

- **Intrusion detection system**—An **intrusion detection system (IDS)** is designed to detect threats. It cannot prevent a threat. A passive IDS will log the event and may provide an alert. An active IDS may modify the environment to block the attack after it is detected. Many IDS systems use definitions the way antivirus software uses signatures. A network-based intrusion detection system (NIDS) provides overall network protection. A host-based intrusion detection system (HIDS) can protect individual systems.

- **Incident response**—When a company is prepared and able to respond to an incident, it has a better chance to reduce the impact. An important step when responding to an incident is containment, which ensures the incident doesn't spread to other systems. An incident response team tries to identify what happened. They look for the vulnerabilities that allowed the incident. They then seek ways to reduce the vulnerability in the future. On the other hand, some companies would like to quickly put the incident behind them. They try to fix the immediate issue without addressing the underlying problem. When you address underlying problems, you reduce the chance of recurring incidents for the same issue.
- **Continuous monitoring**—Security work is never finished. **Continuous monitoring** is necessary. You implement controls and then check and audit to ensure they are still in place. You deploy patches. Later, through compliance audits, you verify that all systems are patched. Through access controls you lock down systems and data. Later, you check to ensure they haven't been modified. You record a wide range of activity in logs and then monitor these logs for trends and suspicious events. Luckily, there are many tools that you can use to audit and monitor systems within a network.
- **Technical controls**—Controls that use technology to reduce vulnerabilities. IT professionals implement the controls and computers enforce them. For example, after an IT professional installs antivirus software, the software prevents infections. Some other examples of **technical controls** include intrusion detection systems, access controls, and firewalls. As you discover new vulnerabilities, you can implement new technical controls.
- **Physical controls**—**Physical controls** prevent unauthorized personnel from having physical access to areas or systems. For example, you should locate servers in server rooms and keep the server room doors locked. Place network devices in wiring closets and keep the wiring closet doors locked. Physical security can also include guards, cameras, and other monitoring equipment. For mobile equipment, such as laptops, you can use cable or hardware locks.

Best Practices for Managing Vulnerabilities Within Your IT Infrastructure

Vulnerabilities are the portion of the threat/vulnerability pair that you can control. Therefore, it's very important to take steps to manage vulnerabilities. Here are some of the best practices you can use to do this:

- **Identify vulnerabilities**—Several tools are available that you can use to identify vulnerabilities. For example, audits and system logs help identify weaknesses. Use all the available tools, and examine all seven domains of the typical IT infrastructure.

- **Match the threat/vulnerability pairs**—The vulnerabilities you want to address first are the ones that have matching threats. Some vulnerabilities may not have a matching threat. If so, the weakness may not need to be addressed. For example, you may have an isolated network used for testing that does not have any access to the Internet. Weaknesses that can be exploited only from Internet threats can't reach this network and may be ignored.

- **Use as many of the mitigation techniques as feasible**—Several mitigation techniques were listed in this section. It's certainly possible to use all of these techniques. Depending on your IT infrastructure, you may use more. With multiple techniques in place, you create multiple layers of security.
- **Perform vulnerability assessments**—Vulnerability assessments can help you identify weaknesses. You can perform them internally or hire external experts to perform them.

Understanding and Managing Exploits

Losses occur when threats exploit vulnerabilities. If you want to reduce losses due to risks, you'll need to have a good understanding of what exploits are and how to manage them. This section covers the following topics:

- What an exploit is
- How perpetrators initiate an exploit
- Where perpetrators find information about vulnerabilities and exploits
- Mitigation techniques
- Best practices for managing exploits within your IT infrastructure

What Is an Exploit?

An **exploit** is the act of taking advantage of a vulnerability. It does so by executing a command or program against an IT system to take advantage of a weakness. The result is a compromise to the system, an application, or data. You can also think of an exploit as an attack executed by code.

In this context, an exploit primarily attacks a public-facing server. In other words, it attacks servers that are available on the Internet. Common Internet servers are:

- Web servers
- Simple Mail Transfer Protocol (SMTP) e-mail servers
- File Transfer Protocol (FTP) servers

Figure 2-2 shows how these public-facing servers are often configured in a network. They are placed within two firewalls configured as a **demilitarized zone (DMZ)**. A DMZ is also known as a *buffer area*, or a *perimeter zone*. The firewall connected to the Internet allows access to these public-facing servers. The firewall connected to the internal network restricts traffic from the Internet.

Since the servers in the DMZ are public facing, they are accessible to anyone with a public Internet Protocol (IP) address. This includes attackers or black-hat hackers.

While internal servers are susceptible to attacks from employees, it isn't common for an employee to use an exploit to attack an internal server. Employees can attack and cause damage. However, it's much easier for an employee to steal data or perform acts of sabotage. An insider usually won't take the time to write a program to attack an internal system. Insiders have the advantage of at least some basic employee privileges and internal knowledge. It's also common that the internal network is trusted, so the company gives less attention to exploits on the internal network.

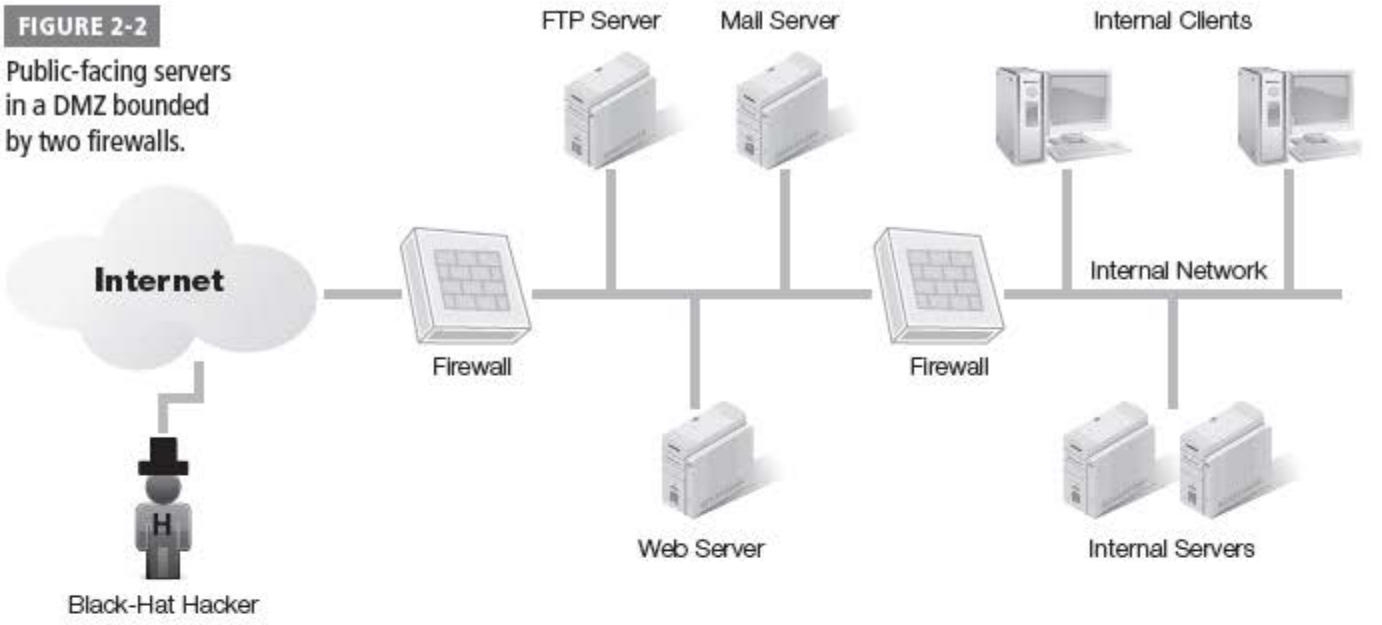


FIGURE 2-2
Public-facing servers in a DMZ bounded by two firewalls.

A **buffer overflow** is a common type of exploit. A buffer overflow can occur when an attacker sends more data or different data than a system or application expects. The vulnerability exists when the system or application is not prepared to reject it. This can cause the system to act unreliably. Additionally, if the exploit's creator is especially skilled, the exploit runs extra instructions, gaining the attacker additional privileges on a system.

Normally, the system will validate data and reject data that isn't expected. Occasionally, a bug allows invalid data to be used.

For example, imagine a simple calculation: X / Y = Z. The program expects the value of X and Y to be provided. It will then divide the two to calculate the value of Z. However, if zero is given as the value of X or Y, Z cannot be calculated. You can't divide anything by zero. If the program didn't check to ensure that X and Y were valid numbers, the program could fail when a user enters zero. If the error isn't handled gracefully, an attacker may be able to exploit the failure.

NOTE
While a divide-by-zero error is simple to explain, it's unlikely this will cause a problem today. Most applications will detect the problem and never try to divide by zero. However, there are many more advanced errors that aren't predicted.

Buffer overflow errors allow attackers to insert additional data. This additional data can be malware that will remain in the system's memory until it's rebooted. It could insert a worm that spreads through the network. It could be code that seeks and destroys data on the system. It could cause the server to shut down and no longer be able to reboot.

When a vendor finds buffer overflow vulnerabilities, it patches the code to prevent the error in the future. You should download this patch and apply it to plug the hole.

The Nimda Virus

The Nimda virus is an example of an older virus that took advantage of a buffer overflow problem in Microsoft's Internet Information Services (IIS). This virus helps explain many of the lessons learned with IT risk management.

First, IIS was installed by default when Windows 2000 Server was installed. Since IIS was installed by default, it often wasn't managed. An unmanaged service is easier to attack.

When the buffer overflow was discovered, Microsoft released a patch. This patch corrected the problem as long as it was applied. However, patch management was in its infancy at that time. Many companies didn't have effective patch management programs and didn't apply patches consistently. Many system administrators concluded incorrectly that because they weren't using IIS, their systems weren't vulnerable. However, because IIS was installed by default, their systems were, in fact, vulnerable.

Nimda was released on the Internet and had a multipronged approach. The buffer overflow allowed it to exploit an IIS system. It had a worm component that allowed it to seek and infect other systems on the internal network. It also looked for other IIS servers on the Internet susceptible to the same buffer overflow. It slowed network activity to a crawl and destroyed data.

Two of the basic security practices that were reinforced by Nimda are:

- **Reduce the attack surface of servers**—Unneeded services and protocols should not be installed. If they were installed, they should be removed. If IIS wasn't installed on a server, it couldn't have been attacked by Nimda.
- **Keep systems up to date**—If IIS servers had been updated with the released patch, they wouldn't have been susceptible to the attack.

Other exploits include:

- **SQL injection attacks**—SQL injection attacks take advantage of dynamic SQL. Many Web sites require users to enter data in a text box or Web address. If the user-supplied data is used directly in a SQL statement, a SQL injection attack can occur. Instead of giving the data that's expected, a SQL injection attack gives a different string of SQL code. This different code can compromise the database. SQL injection attacks are easy to avoid by using parameters and stored procedures that first review the code. However, all database developers aren't aware of the risks.

NOTE

Structured Query Language (SQL) is the language used to query and modify databases. It has specific rules that you must follow. Dynamic SQL is a SQL statement that accepts input from a user directly. For example, the statement may be `SELECT FROM Users Where LName = 'txt.Name'`. In this example, the value of `txt.Name` is retrieved from the text box named *txt.Name* and used when the program is run. Permitting input directly from a user without any input filtering is not recommended.

- **Denial of service (DoS) attacks**—Denial of service (DoS) attacks are designed to prevent a system from providing a service. For example, a **SYN flood attack** is very common. Normally TCP uses a three-way handshake to start a connection. A host sends a packet with the SYN flag set. The server responds with the SYN and ACK flags set. The host then responds with the ACK flag set to complete the handshake. In the SYN flood attack, the host never responds with the third packet. It's as if the host stuck out his hand to shake, the server put his hand out, and then the host pulled his hand away. The server is left hanging. When this is repeatedly done in a short time period, it consumes the server's resources and can cause it to crash.
- **Distributed denial of service (DDoS) attacks**—Distributed denial of service (DDoS) attacks are initiated from multiple clients at the same time. For example, many criminals and attackers run botnets from a command and control center. A botnet controls multiple hosts as *clones* or *zombies*. These clones can be given a command at any time to attack, and they all attack at the same time. The attack could be as simple as constantly pinging the same server. If thousands of clients are pinging a server at the same time, it can't respond to other requests as easily.

How Do Perpetrators Initiate an Exploit?

Most exploits are launched by programs developed by attackers. The attackers create and run the programs against vulnerable computers.

You've probably heard about **script kiddies.** These are attackers with very little knowledge, sometimes just young teenagers. However, they can download scripts and small programs and launch attacks. They don't have to be very intelligent about computers or even about the potential harm they can do. Some programs are so simple, the script kiddie can just enter an IP address and click Go to launch an attack.

However, the attackers most companies are worried about are much more sophisticated. They have programming skills. They know how to target specific servers. They know methods to infiltrate networks. They erase evidence to cover their tracks. They are professional attackers.

Imagine a country hostile to the United States with extensive computer expertise. They could create their own internal secret department with separate divisions. Each division could be assigned specific jobs or tasks. Each of the divisions could work together to launch exploits as soon as they become known. This department could have the following divisions:

- **Public server discovery**—Every system on the Internet has a public IP address. This division could use ping scanners to identify any systems that are operational with public IP addresses. IP addresses are assigned geographically, so servers can also be mapped to geographical locations.

- **Server fingerprinting**—This division could use several methods to learn as much about the discovered server as possible. They can use a ping to identify if the systems are running UNIX or Microsoft operating systems. They can use port scans to identify what ports are open. Based on what ports are open, they can identify the running protocols. For example, port 80 is the well-known port for Hypertext Transfer Protocol (HTTP), so if port 80 is open, HTTP is probably running. If HTTP is running, it is probably a Web server. The department can use other techniques to determine if it's an Apache Web server or an IIS Web server.
- **Vulnerability discovery**—Investigators and hackers in this division could constantly be on the lookout for any new weaknesses. They could just try new things to see what can be done. They could lurk on newsgroups to hear about new bugs that aren't widely known. They could subscribe to professional journals or read blogs by IT security experts. When they discover a vulnerability, they would pass it on to programmers or attackers to exploit.
- **Programmers**—Once vulnerabilities are discovered, programmers can write code or applications to exploit them. It could be just a few lines of code that are embedded into a Web page and downloaded when a user visits the Web site. It could be a virus that is released to exploit the weakness. It could be an application that is installed on zombie computers waiting for the botnet command to attack.
- **Attackers**—Attackers initiate the exploit. For example, attackers may discover a new vulnerability for Apache servers. The attackers may want to target servers in Washington D.C. They could get a list of servers in D.C. running Apache from other divisions. They can then launch an attack on those servers. This group might regularly launch legacy attacks that current patches block. Most systems will be patched, but if group members find an unpatched system, they can exploit it. Say they launch an attack on 10,000 computers. Even if they have only a 1 percent success rate, they've exploited 100 computers.

> **NOTE**
>
> Attackers often use diversion when launching attacks. Instead of launching the attack from their own computer, they will often take control of one or more other computers on the Internet. They then direct the attack from that remote-controlled computer.

This secret department in a hostile country is presented as fictitious. However, cyberattacks from one country against another are not fiction. The news reports cyberattacks regularly. Operation Aurora and Operation Shady RAT (mentioned previously in this chapter) are two recent examples. If you wanted to commit cyberwarfare against a hostile country, how would you do so? It's very possible you would design a similar department with similar divisions.

Even if it is a single perpetrator launching an attack, the steps listed above would be separated. The attacker would take time through reconnaissance to learn as much about a target as possible. The attacker may develop a program to automate the attack. The actual attack is usually quick.

It's important to realize that attackers very often spend 100 percent of their work time on attacks. Since many attacks often return significant amounts of money, they aren't shy about working more than 40 hours a week. They take time to discover targets. They take time to identify weaknesses. They take time to plan the attacks. When the opportunity presents itself, they swoop in and attack just as quickly as an owl will attack a field mouse.

Where Do Perpetrators Find Information About Vulnerabilities and Exploits?

There are a surprising number of sources for perpetrators to learn about vulnerabilities and exploits. A primary source is from security professionals sharing information with each other.

Of course, when security professionals write about or discuss an exploit, the danger is that they are educating the enemy. This leads some people to say that the weaknesses shouldn't be discussed at all. However, when nothing is said, systems are attacked without IT professionals having a clue about the vulnerabilities.

The general mindset that currently prevails is that the vulnerabilities should be discussed with a focus on mitigation. In other words, don't publicly share the details on how to exploit a vulnerability. However, freely share the details on how to prevent the vulnerability.

Even sharing details about how to prevent a vulnerability provides the attackers with information. They can use this to learn the weakness and exploit it. However, the alternative is worse. If information on how to reduce the weakness isn't shared, more systems will be wide open.

The following list identifies some sources that attackers can use to gain information:

- **Blogs**—Many security professionals regularly blog about their findings. When they suspect vulnerabilities, they often discuss them. Many full-time security professionals are cautious about what they post. They realize they have a mixed audience and try to avoid giving too many details.
- **Forums**—IT and security professionals often share ideas on different forums. Sometimes users have problems they don't understand, so they post their problems on the forum. Some of these problems expose vulnerabilities that can be exploited.
- **Security newsletters**—Many security newsletters are regularly released to anyone on the e-mail list. Anyone can sign up. While companies use newsletters to advertise and promote their products, they also provide valuable content. This includes content about threats and vulnerabilities. Even the newsletters published by the U.S. government can be used by attackers. Some of these newsletters are discussed later in this chapter, including how to subscribe.
- **2600: Hacker quarterly**—You can subscribe to this or pick up the printed version in some bookstores. They frequently include code and details that can be used to exploit vulnerabilities.
- **Common Vulnerabilities and Exposures (CVE) list**—The CVE is discussed in more detail later in this chapter. When someone discovers a vulnerability, it can be submitted to the MITRE Corporation for inclusion in this list. The entry about the vulnerability will include information on resources for more details.

- **Reverse engineering**—Patch Tuesday was mentioned earlier as the day that Microsoft releases patches. It is the second Tuesday of every month. The day after is known as **Exploit Wednesday** by some. Attackers often reverse engineer the patches to discover the vulnerability. Once the weakness is understood, exploits are written to attack the weakness.

A good philosophy to adopt is this: If a known vulnerability exists, a bad guy knows about it. Remember, it only takes one bad guy who knows about the vulnerability to attack an unprotected system. You must protect all of the systems to stay protected.

> **NOTE**
>
> Many corporate clients of Microsoft have advance notice that patches will be released. This allows the companies to perform advance testing of the patches. When the patches are formally released, the companies are ready to apply them immediately.

Mitigation Techniques

Mitigation techniques are the individual steps you need to take to protect any system that is vulnerable. Together these steps are often referred to as **hardening a server.** Hardening a server makes it more secure from the default installation.

Some of the specific mitigation techniques you can take to protect public-facing servers are:

- **Remove or change defaults**—If an operating system or application has any defaults, ensure they are removed or changed as soon as the system is installed. As an example, change default passwords to secure passwords. It's also common to change the name of privileged accounts such as the Administrator account. This thwarts attempts to guess the password.
- **Reduce the attack surface**—The **attack surface** refers to how much can be attacked on a server. For example, if 10 services are running on a server, but you only need seven, you reduce the attack surface by disabling the three unneeded services. The overall attack surface is reduced by removing all unneeded services and protocols. If a service isn't needed, it should be disabled. If the protocol isn't needed, it should be removed. Every service and protocol that is running adds more risk to the system. When you remove unneeded ones, you reduce the risk without impacting the quality of the service.
- **Keep systems up to date**—Use a patch management system to ensure that systems are patched. Patches should be applied as quickly as possible after they are released. Every hour that passes gives the attackers more time to reverse engineer the patch and begin their attacks. Compliance audits ensure that patches are consistently applied to all systems.
- **Enable firewalls**—Firewalls filter traffic coming into a network. DMZs use firewalls to create network buffer areas. You can also enable host-based firewalls on each server as an added layer of protection.
- **Enable intrusion detection systems (IDSs)**—An active IDS can detect attacks and take steps to stop them.

- **Enable intrusion prevention systems (IPSs)**—An **intrusion prevention system (IPS)** is placed in-line with traffic. It can detect and block malicious traffic. This prevents attacks from reaching the internal network.
- **Install antivirus software**—Antivirus software should be installed on all systems, including servers, before they are connected to the network. Many servers require different versions of antivirus software. For example, a Microsoft Exchange mail server needs a specialized version of antivirus software so the mail stores can be examined.

Best Practices for Managing Exploits Within Your IT Infrastructure

There are several best practices you can use to reduce your risks from exploits. Many of these are directly related to basic risk management practices:

- **Harden servers**—Methods were mentioned in the previous section. They include basic steps such as reducing the attack surface and keeping systems up to date.
- **Use configuration management**—Ensure systems are configured with consistent security settings. Use security baselines to ensure systems are configured the same way. A security baseline can come from an image created with a tool like Symantec's Ghost. You can also achieve it by applying settings to all systems with technology like Microsoft's Group Policy. Perform compliance audits to ensure that systems stay configured the same way.
- **Perform risk assessments**—Performing risk assessments allows you to learn about the relevant threats and vulnerabilities. You can then identify and evaluate countermeasures.
- **Perform vulnerability assessments**—Vulnerability assessments were mentioned earlier in this chapter. You can also use them as a best practice to manage exploits.

U.S. Federal Government Risk Management Initiatives

The U.S. federal government has taken many steps to help companies manage IT risks. The initiatives covered in this section are:

- The National Institute of Standards and Technology (NIST)
- The Department of Homeland Security (DHS)
- The National Cybersecurity and Communications Integration Center (NCCIC)
- The United States Computer Emergency Readiness Team (US-CERT)
- The MITRE Corporation and the CVE list

Figure 2-3 shows the relationships among many of these organizations. There are two primary paths: One is under the U.S. Department of Commerce. The other is under the Department of Homeland Security.

NIST is directly under the Department of Commerce. The Information Technology Laboratory (ITL), part of NIST, publishes special publications. The Department of Homeland Security includes the Office of Cybersecurity and Communications.

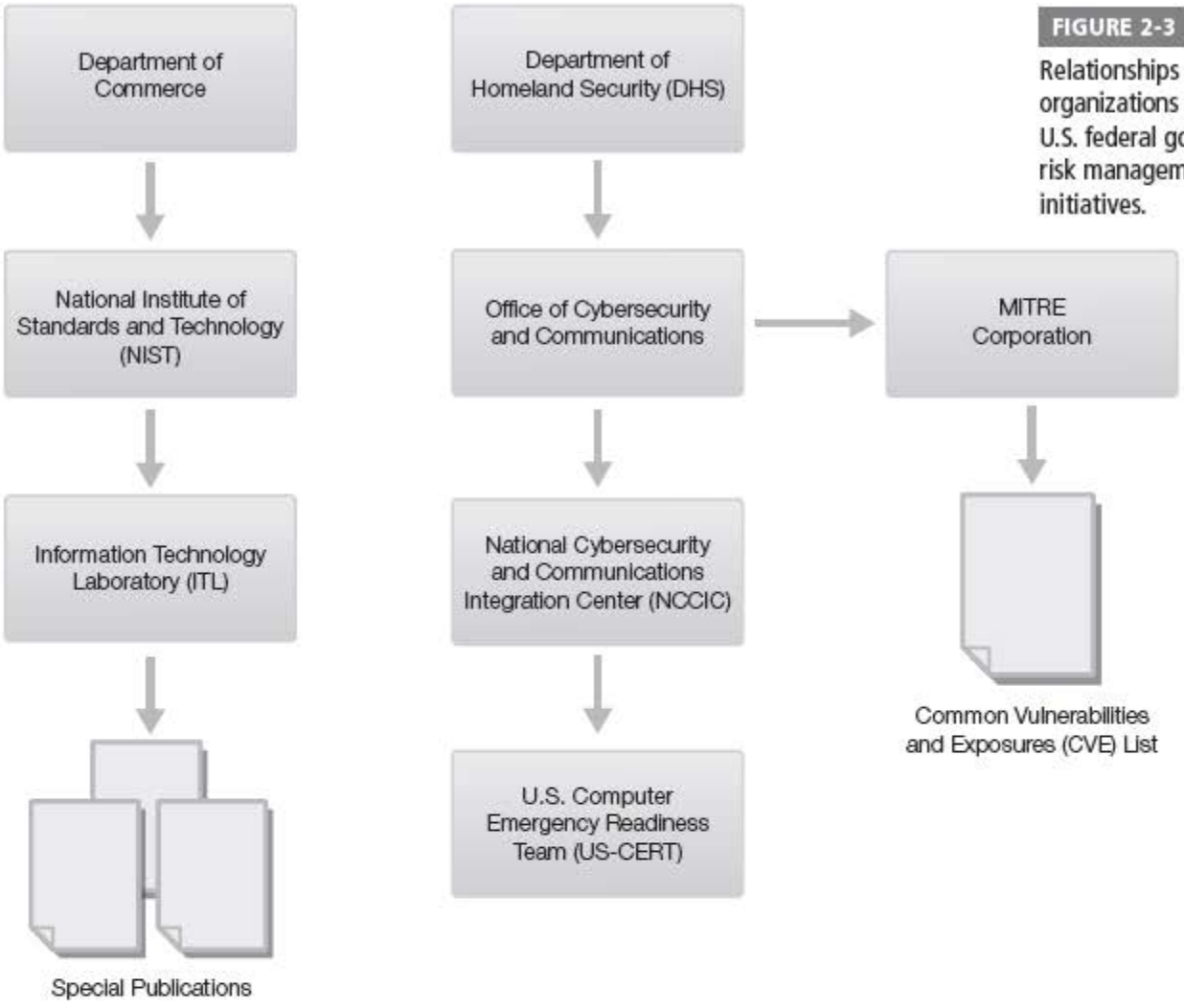


FIGURE 2-3
Relationships among organizations involved in U.S. federal government risk management initiatives.

Within this office is the National Cybersecurity and Communications Integration Center. The Office of Cybersecurity and Communications provides funding for the civilian company the MITRE Corporation. MITRE maintains the Common Vulnerabilities and Exposures list. The US-CERT is located within the NCCIC.

National Institute of Standards and Technology

The **National Institute of Standards and Technology (NIST)** is a division of the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness. It does this by advancing measurement science, standards, and technology.

NIST includes the Information Technology Laboratory (ITL). ITL develops standards and guidelines. The goal is improved security and privacy of information on computer systems.

> **NOTE**
> ITL and ITIL are two different programs. The Information Technology Infrastructure Library (ITIL) was developed by the United Kingdom (UK). It is managed by the UK Office of Government Commerce (OGC). ITIL is a collection of books that provides guidance and best practices for the successful operation of IT. The ITL managed by NIST is a U.S. program.

The Special Publication 800 (SP 800) series includes several reports that document ITL's work. It includes research, guidance, and outreach efforts in computer security. It is intended to be a collaborative effort combining the work of industry, government, and academic organizations. Many of the publications in the SP 800 series are available on the Internet. NIST has revised many of these documents and the number doesn't reflect the relative date of the current version.

The following list includes some of these:

- SP 800-153, "Guidelines for Securing Wireless Local Area Networks (WLANs)"
- SP 800-124, "Guidelines for Managing the Security of Mobile Devices in the Enterprise"
- SP 800-123, "Guide to General Server Security"
- SP 800-122, "Guidelines for Protecting the Confidentiality of Personally Identifiable Information (PII)"
- SP 800-121, "Guide to Bluetooth Security"
- SP 800-119, "Guidelines for Secure Deployment of IPv6"
- SP 800-115, "Technical Guide to Information Security Testing and Assessment"
- SP 800-100, "Information Security Handbook: A Guide for Managers"
- SP 800-94, "Guide to Intrusion Detection and Prevention Systems"
- SP 800-83, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops"
- SP 800-61, "Computer Security Incident Handling Guide"
- SP 800-55, "Performance Measurement Guide for Information Security"
- SP 800-51, "Guide to Using Vulnerability Naming Schemes"
- SP 800-50, "Building an Information Technology Security Awareness and Training Program"
- SP 800-40, "Creating a Patch and Vulnerability Management Program"
- SP 800-30, "Guide for Conducting Risk Assessments"
- SP 800-12, "An Introduction to Computer Security: The NIST Handbook"

NOTE

You can access the full list of Special Publications including links to all of them from the NIST Web site at *http://csrc.nist.gov/publications/PubsSPs.html*.

Department of Homeland Security

The **Department of Homeland Security (DHS)** is responsible for protecting the United States from threats and emergencies. Its primary goal is to keep America safe, and it focuses on protecting the United States from terrorist attacks. DHS is also responsible for responding to natural disasters, such as hurricanes and earthquakes.

Congress passed the Homeland Security Act of 2002 in November 2002. This act established the DHS. The Homeland Security Act of 2002 and the DHS were created in response to the terrorist bombings of September 11, 2001.

The DHS includes many agencies. Some of them are:

- United States Secret Service
- United States Coast Guard
- U.S. Immigration and Customs Enforcement
- U.S. Customs and Border Protection
- Federal Emergency Management Agency

National Cybersecurity and Communications Integration Center

The **National Cybersecurity and Communications Integration Center (NCCIC)** operates within the DHS. It works together with private, public, and international parties to secure cyberspace and America's cyberassets.

Previously, cybersecurity was scattered in different departments. Today, the NCCIC serves as the central point of contact. The NCCIC oversees several programs:

- **National Cyber Awareness System**—This is an e-mail alert system that allows you to subscribe to different types of e-mails.
- **United States Computer Emergency Readiness Team (US-CERT) Operations**—This division is tasked with analyzing and reducing cyberthreats and vulnerabilities. As issues become known, US-CERT disseminates information and can coordinate incident response activities. See the following section for more information about US-CERT.
- **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)**—This group works to reduce risks to critical infrastructure sectors. This includes roads, water, communications, energy, and more.

> **NOTE**
>
> *Cyber* generally refers to any computer assets, but usually refers to assets on the Internet. The global network of computers on the Internet is commonly referred to as *cyberspace*. *Cyberwarfare*, or cyberwar, refers to the attacks and counterattacks carried out against other countries or other companies.

US Computer Emergency Readiness Team

The **United States Computer Emergency Readiness Team (US-CERT)** is a part of the NCCIC. US-CERT's primary mission is to provide response support and defense against cyberattacks. Its focus is on providing support for the federal civil executive branch of government, or any sites with a .gov domain name. However, US-CERT also collaborates and shares information with several other entities, including:

- State and local governments
- International partners
- Other federal agencies
- Other public and private sectors

> **NOTE**
> One of the great benefits of the National Cyber Awareness System is that the e-mails don't include advertisements. Also, because they are from the U.S. government, the information is not slanted to sell or promote specific products.

Information gathered by US-CERT is shared with the public through the National Cyber Awareness System. These include their Web site, mailing lists, and Really Simple Syndication (RSS) channels.

You can sign up to receive e-mails and alerts from US-CERT from this link: *http://www.us-cert.gov/mailing-lists-and-feeds/*. You can sign up for any or all of the following feeds:

- **Alerts**—These alerts include timely information about current security issues, vulnerabilities, and exploits. Alerts are released as needed. They are written for system administrators and experienced users. You can view past alerts at *http://www.us-cert.gov/ncas/alerts*.
- **Bulletins**—These bulletins provide summaries of security issues and vulnerabilities from the previous week. They are published weekly and are written for system administrators and experienced users. You can view past bulletins at *http://www.us-cert.gov/ncas/bulletins*.
- **Current Activity**—These provide information about high-impact types of security activity. Depending on current threats, these e-mails can be sent several times a day or several times a week. You can view past updates at *http://www.us-cert.gov/ncas/current-activity/*.
- **Tips**—These tips are targeted to home, corporate, and new users. They are published every two weeks and provide tips on many security topics. You can view past security tips at *http://www.us-cert.gov/ncas/tips*.

The MITRE Corporation and the CVE List

> **NOTE**
> MITRE is an acronym, but the initials are not relevant. Many of the original employees came from the Massachusetts Institute of Technology (MIT). These employees work on research and engineering (RE). However, MITRE is not a part of MIT.

The MITRE Corporation manages four Federally Funded Research and Development Centers (FFRDCs). These FFRDCs conduct research for several major departments of the U.S. government.

The MITRE Corporation maintains the CVE list. MITRE is the editor of the list and is responsible for assigning numbers. The U.S. Department of Homeland Security sponsors the CVE.

Common Vulnerabilities and Exposures (CVE) List

The CVE is an extensive list of known vulnerabilities and exposures. As new discoveries are made, they are submitted as candidates for the list. The primary benefit of the list is standardized naming and descriptions.

Before the CVE, one company may have addressed a problem as Exploit234a. The same problem could have been addressed by another company as X42A. Both companies may have published papers regarding the same problem, but it was difficult to determine if one problem was different from the other.

The CVE provides one name for any single vulnerability or exposure. The format is CVE-yyyy-nnnn, where *yyyy* is the year the vulnerability was added to the list and *nnnn* is a unique number for the year. Effective January 1, 2014, the number can include up to six digits. Previously, only four digits were allowed, limiting this to 9,999 CVE-IDs. With six digits, MITRE can assign up to 99,999 CVE-IDs. CVEs include a brief description. They also include one or more references users can access for more information. The following example shows a CVE from 2013:

- **Name**—CVE-2013-1247
- **Description**—Cross-site scripting (XSS) vulnerability in the wireless configuration module in Cisco Prime Infrastructure allows remote attackers to inject arbitrary Web script or Hypertext Markup Language (HTML) via an SSID that is not properly handled during display of the Extensible Markup Language (XML) windowing table, also known as Bug ID CSCuf04356.
- **References**—URL: *http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-1247*

NIST uses the CVE names and descriptions in the National Vulnerability Database (NVD). The NVD listings include the same information from the CVE but add in impact and severity scores. This page (*http://cve.mitre.org/cve/*) includes links to search for the CVE on MITRE's CVE list or on NIST's NVD list.

Standard for Information Security Vulnerability Names

The CVE is considered the standard for information security vulnerability names. MITRE launched the CVE in 1999, and it was quickly embraced. Some of the relevant milestones are:

- **Year 2000**—Over 40 products were declared compatible with CVE. CVE is used by 29 organizations.
- **Year 2001**—Over 300 products and services were declared compatible. CVE is used by more than 150 companies.
- **Year 2002**—NIST recommends the use of CVE by U.S. agencies. NIST SP 800-51, "Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme," is released. SP 800-51 was updated and renamed in 2011. The current name is "Guide to Using Vulnerability Naming Schemes."
- **Year 2003**—The CVE Compatibility process is started. This allows products and services to achieve official compatibility status.
- **Year 2004**—The U.S. Defense Information Systems Agency (DISA) requires use of products that use CVE identifiers.
- **Year 2007**—NVD implemented several upgrades to the CVE-based database. These increased usability and improved the scoring system. Many other entities have since adopted the NVD. This has increased the use of the CVE as a standard.

The FBI/SANS Top 20 List of the Most Critical Internet Security Vulnerabilities also references the CVE list.

CHAPTER SUMMARY

Threats are always present and can't be eliminated. You reduce the potential for a threat to do harm, or you reduce the impact of a threat, but not the threat itself. However, you can take many steps to reduce vulnerabilities. The most important vulnerabilities are those that are likely to match up as a threat/vulnerability pair. Once you identify likely threat/vulnerability pairs, you can implement mitigation techniques.

The U.S. federal government has many resources that organizations can use to manage risk. The National Institute of Standards and Technology (NIST) has published several Special Publications. The SP 800 series includes many publications targeted for IT security. The Department of Homeland Security also has many divisions focused on IT security. Their resources are freely available to IT and security professionals.

KEY CONCEPTS AND TERMS

- Attack surface
- Buffer overflow
- Configuration management
- Continuous monitoring
- Demilitarized zone (DMZ)
- Denial of service (DoS) attacks
- Department of Homeland Security (DHS)
- Distributed denial of service (DDoS) attacks
- Exploit
- Exploit Wednesday
- Hardening a server
- Intentional threats
- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- National Cybersecurity and Communications Integration Center (NCCIC)
- National Institute of Standards and Technology (NIST)
- Patch management
- Patch Tuesday
- Physical controls
- Principle of least privilege
- Principle of need to know
- Script kiddies
- Security policy
- Separation of duties
- SQL injection attacks
- SYN flood attack
- Technical controls
- Threat/vulnerability pair
- Unintentional threats
- United States Computer Emergency Readiness Team (US-CERT)
- Version control

CHAPTER 2 ASSESSMENT

1. What is a security policy?
   A. A rigid set of rules that must be followed explicitly to be effective
   B. A technical control used to enforce security
   C. A physical control used to enforce security
   D. A document created by senior management that identifies the role of security in the organization

2. You want to ensure that users are granted only the rights to perform actions required for their jobs. What should you use?
   A. Principle of least privilege
   B. Principle of need to know
   C. Principle of limited rights
   D. Separation of duties

3. You want to ensure that users are granted only the permissions needed to access data required to perform their jobs. What should you use?
   A. Principle of least privilege
   B. Principle of need to know
   C. Principle of limited rights
   D. Principle of limited permissions

4. Which of the following security principles divides job responsibilities to reduce fraud?
   A. Need to know
   B. Least privilege
   C. Separation of duties
   D. Mandatory vacations

5. What can you use to ensure that unauthorized changes are not made to systems?
   A. Input validation
   B. Patch management
   C. Version control
   D. Configuration management

6. What are two types of intrusion detection systems?
   A. Intentional and unintentional
   B. Natural and man-made
   C. Host-based and network-based
   D. Technical and physical

7. A technical control prevents unauthorized personnel from having physical access to a secure area or secure system.
   A. True
   B. False

8. What allows an attacker to gain additional privileges on a system by sending unexpected code to the system?
   A. Buffer overflow
   B. MAC flood
   C. Input validation
   D. Spiders

9. What is hardening a server?
   A. Securing it from the default configuration
   B. Ensuring it cannot be powered down
   C. Locking it in a room that is hard to access
   D. Enabling necessary protocols and services

10. Which of the following steps could be taken to harden a server?
    A. Removing unnecessary services and protocols
    B. Keeping the server up to date
    C. Changing defaults
    D. Enabling local firewalls
    E. All of the above

11. Which government agency includes the Information Technology Laboratory and publishes SP 800-30?
    A. NIST
    B. DHS
    C. NCCIC
    D. US-CERT

12. ITL and ITIL are different names for the same thing.
    A. True
    B. False

13. Which U.S. government agency regularly publishes alerts and bulletins related to security threats?

A. NIST
B. FBI
C. US-CERT
D. The MITRE Corporation

14. The CVE list is maintained by _____.

15. What is the standard used to create Information Security Vulnerability names?

A. CVE
B. MITRE
C. DISA
D. CSI

CHAPTER 3

Maintaining Compliance

MANY LAWS AND REGULATIONS ARE IN PLACE regarding the protection of information technology (IT) systems. Companies have a requirement to comply with the laws that apply to them. The first step is to understand the laws. You're not expected to be a lawyer, but you should understand the basics of relevant laws.

Once you have an idea of which laws and regulations apply, you can then dig in deeper to ensure your organization is in compliance. The cost of not complying can sometimes be expensive. Fines can be in the hundreds of thousands of dollars. Some offenses can result in jail time.

Chapter 3 Topics

This chapter covers the following topics and concepts:

- What U.S. compliance laws exist
- What some relevant regulations related to compliance are
- What organizational policies for compliance should be considered
- What standards and guidelines for compliance exist

Chapter 3 Goals

When you complete this chapter, you will be able to:

- Define compliance
- Describe the purpose of FISMA
- Identify the purpose and scope of HIPAA
- Describe GLBA and SOX, and the impact for IT
- Describe the purpose of FERPA

- Identify the purpose and scope of CIPA
- List some federal entities that control regulations related to IT
- Describe the purpose of PCI DSS
- Describe the contents of SP 800-30
- Describe the purpose of COBIT
- Describe the purpose of ISO and identify some relevant security standards
- Identify the purpose of ITIL
- Identify the purpose of CMMI

U.S. Compliance Laws

Many laws exist in the United States related to information technology (IT). Companies affected by the laws are expected to comply with the laws. This is commonly referred to as **compliance**.

Many organizations have internal programs in place to ensure they remain in compliance with relevant laws and regulations. These programs commonly use internal audits. They can also use certification and accreditation programs. When compliance is mandated by law, external audits are often done. These external audits provide third-party verification that the requirements are being met.

An old legal saying is "ignorance is no excuse." In other words, you can't break the law and then say "I didn't know." The same goes for laws that apply to any organization. It's important for any organization to know what the relevant laws and regulations are.

You aren't expected to be an expert on any of these laws. However, as a manager or executive, you should be aware of them. You can roll any of the relevant laws and regulations into a compliance program for more detailed checks.

This section covers the following U.S. laws:

- Federal Information Security Management Act (FISMA) 2002
- Health Insurance Portability and Accountability Act (HIPAA) 1996
- Gramm-Leach-Bliley Act (GLBA) 1999
- Sarbanes-Oxley Act (SOX) 2002
- Family Educational Rights and Privacy Act (FERPA) 1974
- Children's Internet Protection Act (CIPA) 2000

Federal Information Security Management Act

The **Federal Information Security Management Act (FISMA)** was passed in 2002. Its purpose is to ensure that federal agencies protect their data. It assigns specific responsibilities for federal agencies.

Agencies are responsible for:

- **Protecting systems and data**—Agency heads are responsible for all the systems and data in their agencies.
- **Complying with all elements of FISMA**—FISMA includes details on how to protect systems and data. You must inventory systems. You must also do risk assessments to categorize systems and data. You can use different security controls based on risk levels. Systems must go through a certification and accreditation process.
- **Integrating security in all processes**—Use security throughout the agency. Do continuous monitoring to ensure the systems stay secure.

FISMA requires annual inspections. Each year, agencies must have an independent evaluation of their program. The goal is to determine the effectiveness of the program. These evaluations are to include:

- **Testing for effectiveness**—Policies, procedures, and practices are to be tested. This evaluation doesn't test every policy, procedure, and practice. Instead, a representative sample is tested. What is tested should be a realistic sample.
- **An assessment or report**—This report identifies the agency's compliance. It lists compliance with FISMA. It also lists compliance with other standards and guidelines.

Health Insurance Portability and Accountability Act

The **Health Insurance Portability and Accountability Act (HIPAA)** was passed in 1996. It ensures that health information data is protected. Before HIPAA, personal medical information was often available to anyone. Security to protect the data was lax, and the data was often misused.

The CSI Computer Crime and Security Survey of 2010/2011 identifies many of the trends in IT security. Some of this data helps to show the impact of HIPAA. The following data was gathered from survey respondents:

- Only 6.6 percent were in the health services industry.
- More than 51 percent had to comply with HIPAA.
- HIPAA applies more than any other single law or regulation.

> **NOTE**
>
> HIPAA may sound as if it applies only to the health care industry, but that's not true. Some employers offer health insurance, whose applications may include health information. Health plan entities such as Medicaid that help pay for medical coverage must also be compliant. So must medical records that insurance agents must check.

If your organization handles health information, HIPAA applies. This makes the definition of health information very important. HIPAA defines health information as any data that:

- Is created or received by:
  - Health care providers
  - Health plans
  - Public health authorities
  - Employers
  - Life insurers
  - Schools or universities
  - Health care clearinghouses
- And relates to the health of an individual, including:
  - Past, present, or future health
  - Physical health, mental health, or condition of an individual
  - Past, present, or future payments for health care

NOTE

Title I of HIPAA relates to insurance portability. It identifies rules for insurance plans. For example, when an employee changes jobs, HIPAA helps employees retain insurance. Title I rules aren't related to IT compliance. Only Title II of HIPAA covers the protection of data.

Title II of HIPAA includes a section titled "Administrative Simplification." This section includes the requirements and standards of HIPAA for IT. It includes:

- **Security standards**—Every organization that handles health information must protect it. Companies must also protect systems that handle the information. This includes any health data the organization creates, receives, or sends. Specific standards are to be used for:
  - Storage of data
  - Use of data
  - Transmission of data
- **Privacy standards**—Data must not be shared with anyone without the express consent of the patient. If you've ever gone to a doctor's office or hospital, you've probably signed a consent form. It also informs you of practices used to keep your health information private.
- **Penalties**—Penalties can be levied if the rules aren't followed:
  - *Mistakes*—Fines can be $100 per violation and up to $25,000 per year for mistakes.
  - *Knowingly obtaining or releasing data*—Penalties can be as high as $50,000 and one year in prison.
  - *Obtaining or disclosing data under false pretenses*—Penalties can be as high as $100,000 and five years in prison.
  - *Obtaining or disclosing data for personal gain or malicious harm*—Penalties can be as high as $250,000 and 10 years in prison.

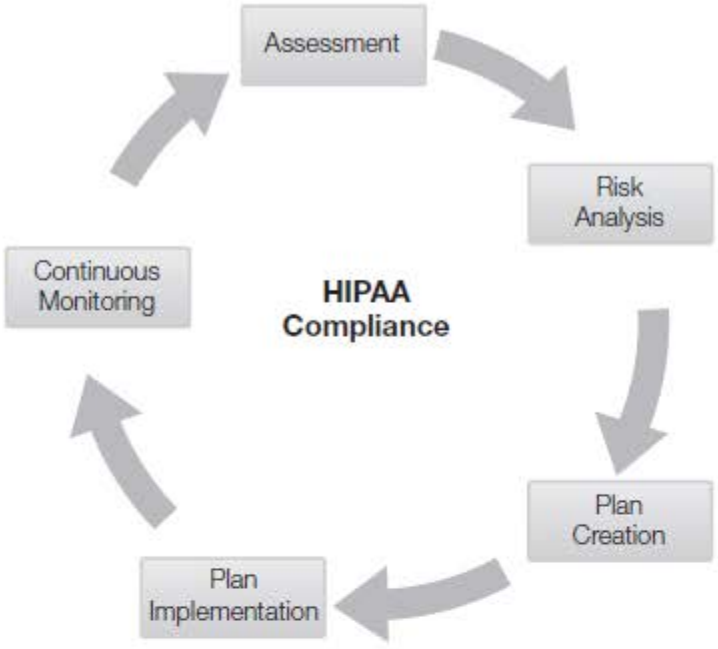


FIGURE 3-1
HIPAA compliance.

If your organization includes data covered by HIPAA, it's important to have a plan. Figure 3-1 shows the process of creating a HIPAA compliance plan:

- **Assessment**—An assessment helps you identify if your organization is covered by HIPAA. If it is, you then identify what data you need to protect.
- **Risk analysis**—A risk analysis helps to identify the risks. In this phase, you analyze how your organization handles data. For example, do you only store data or do you also transfer it electronically?
- **Plan creation**—After you identify the risks, you create a plan. This plan includes methods to reduce the risk.
- **Plan implementation**—You put the plan into place.
- **Continuous monitoring**—Security in depth requires continuous monitoring. Monitor regulations for changes. Monitor risks for changes. Monitor the plan to ensure it is still used.
- **Assessment**—Conduct regular reviews. These ensure the organization remains in compliance.

Gramm-Leach-Bliley Act

The **Gramm-Leach-Bliley Act (GLBA)** was passed in 1999. It is also known as the Financial Services Modernization Act. GLBA is broad in scope. Most of it relates to how banking and insurance institutions can merge.

However, two parts of GLBA are relevant to IT security. They apply to financial institutions in the United States. They are:

- **Financial Privacy Rule**—This rule requires companies to notify customers about their privacy practices. You've probably received a notification from your bank. If you have a credit card, you received one from the credit card company. It explains how the bank or company collects and shares data.
- **Safeguards Rule**—Companies must have a security plan to protect customer information. This plan should ensure data isn't released without authorization. It should also ensure data integrity. Companies are responsible to ensure risk management plans are used. All employees must be trained on security issues.

Sarbanes-Oxley Act

The **Sarbanes-Oxley Act (SOX)** was passed in 2002. This law applies to any company that is publicly traded. It is designed to hold executives and board members personally responsible for financial data. If the data is not accurate, they can be fined and go to jail.

The goal is to reduce fraud. Because individuals can be held liable, there is more pressure to ensure the reported data is accurate. Chief executive officers (CEOs) and chief financial officers (CFOs) must be able to:

- Verify accuracy of financial statements.
- Prove the statements are accurate.

Most of SOX is outside the direct scope of IT. However, Section 404 has some elements that are directly related. Section 404 pertains to the accuracy of data. It requires that a company use internal controls to protect the data.

Section 404 also requires reports from both internal and external auditors to verify compliance. For many companies, the cost of the audits represents the biggest impact of this law.

NOTE

SOX was passed in response to several large scandals. In these scandals, executives deliberately misled the public. Investors lost billions of dollars. For example, Enron was reportedly worth over $100 billion in 2000. It went bankrupt in 2001. It was later determined that the failure was due to fraud and corruption. Many senior officers and board members were directly involved.

Family Educational Rights and Privacy Act

The **Family Educational Rights and Privacy Act (FERPA)** was passed in 1974. It has been amended at least nine times since then. The goal is to protect the privacy of student records. This includes education data and health data.

FERPA applies to all schools that receive any funding from the U.S. Department of Education. This includes:

- Any state or local educational agency
- Any institution of higher education
- Any community college
- Any school or agency offering a preschool program
- Any other education institution

FERPA grants rights to parents of students under 18. The parent can inspect records and request corrections. When the student reaches 18, these rights pass to the student.

All personally identifiable information (PII) about the student must be protected. Schools usually need permission from either the parent or the student to release PII.

There are a few exceptions to when PII can be accessed or released:

- Some school officials may view records.
- Data can be transferred to a new school if the student is transferred.
- Data can be transferred when some types of financial aid are used.
- Accrediting organizations can access data.
- Data can be accessed when required by a court.
- Data can be accessed for health and safety emergencies.

NOTE

PII is a common term used with information security. PII is any data that can be used to identify a person. PII can be a name, a Social Security number, biometric data, or any data used to identify a person. Several laws and regulations specify that PII must be protected.

Children's Internet Protection Act

The **Children's Internet Protection Act (CIPA)** was passed in 2000. It is designed to limit access to offensive content from school and library computers. Any school or library that receives funding from the E-Rate program is covered under CIPA.

CIPA requires that schools and libraries:

- Block or filter Internet access to pictures that are:
  - Obscene
  - Child pornography
  - Harmful to minors (if the computers are accessed by minors)
- Adopt and enforce a policy to monitor online activity of minors
- Implement an Internet safety policy addressing:
  - Access by minors to inappropriate content
  - Safety and security of minors when using e-mail and chat rooms
  - Unauthorized access
  - Unlawful activities by minors online
  - Unauthorized use of minors' personal information
  - Measures restricting minors' access to harmful materials

NOTE

The E-Rate program is a program under the Federal Communications Commission. It provides discounts to most schools and libraries for Internet access. Discounts range from 20 percent to 90 percent of the actual costs.

Some of these terms are difficult to define, such as what is obscene or harmful to minors. CIPA includes a definitions section that identifies other specific sections of U.S. code where some of these terms are defined.

Using Proxy Servers to Limit Content

Most organizations use proxy servers as gateways to access the Internet. An organization configures its computers to use the proxy server. The proxy receives the request, retrieves the Web page from the Internet, and then serves the page to the client.

Proxy servers improve the level of service to clients. You can also use them to filter content. If an organization doesn't want employees to access certain content, the proxy server can block the requests to specific Web sites.

Third-party companies maintain lists of Web sites based on their content. They then sell subscriptions to these lists to any organization that wants them. For example, a company may want to restrict access to gambling sites from a work computer. The gambling list can be purchased and installed on the proxy server. The company can then block any attempts to access these sites.

Proxy servers also have the ability to log attempts by users to access unapproved sites. When a site is blocked, the user will often see a message like: "Warning. Access to this site is restricted by the acceptable use policy. Your activity is being monitored."

Similarly, schools or libraries can use proxy servers to filter content. The technology is widely available.

CIPA was challenged on freedom of speech grounds. The U.S. Supreme Court upheld the law in June 2003. All libraries were given until early 2004 to comply. At this point, it's expected that any school or library accepting E-Rate funds is complying with CIPA.

Regulations Related to Compliance

In addition to laws, there are several regulations that have created different U.S. entities. Most of these entities operate at the federal level.

Some of these entities have a direct impact on information technology (IT) initiatives for most companies. Others are related only to companies engaged in specific activities. Organizations covered in this section are:

- Securities and Exchange Commission (SEC)
- Federal Deposit Insurance Corporation (FDIC)
- Department of Homeland Security (DHS)
- Federal Trade Commission (FTC)
- State Attorney General (AG)
- U.S. Attorney General (U.S. AG)

Securities and Exchange Commission

The **Securities and Exchange Commission (SEC)** is a federal agency. It is charged with regulating the securities industry. This includes any sales or trades of securities. Securities include stocks, bonds, and options.

If your company is involved with the sale or trade of securities, you should be aware of some laws. They are:

- Securities Act of 1933
- Securities Exchange Act of 1934
- Trust Indenture Act of 1939
- Investment Company Act of 1940
- Investment Advisors Act of 1940
- Sarbanes-Oxley Act of 2002
- Dodd-Frank Act of 2010

Many of these laws also apply if your company is a publicly traded company. A *publicly traded company* is any company that has stock that outside investors can buy and sell.

Federal Deposit Insurance Corporation

The **Federal Deposit Insurance Corporation (FDIC)** is a federal agency. It was created in 1933. The primary goal is to promote confidence in U.S. banks. The FDIC was created as a direct result of the bank failures that occurred in the 1920s and early 1930s. These failures led to the Great Depression.

Funds in any bank insured by the FDIC are guaranteed. Depositors will not lose their money even if the bank goes bankrupt. The purpose is to prevent a run on a bank. A "run on a bank" occurs when many depositors rush to withdraw their money.

Currently, funds for any individual depositor are insured to $250,000. The National Credit Union Administration (NCUA) covers credit unions. It also insures deposits up to $250,000.

Department of Homeland Security

The Department of Homeland Security (DHS) is a federal agency. It is responsible for protecting the United States from terrorist attacks. It is also charged with responding to natural disasters.

The DHS was formed in 2002 as a direct response to the terrorist attacks of September 11, 2001. It includes several divisions that are related to IT. These include:

- Office of Cybersecurity and Communications
- National Cybersecurity and Communications Integration Center (NCCIC)
- United States Computer Emergency Readiness Team (US-CERT)

Federal Trade Commission

The **Federal Trade Commission (FTC)** is a federal agency. It was created in 1914. The primary goal is to promote consumer protection, but this has changed over the years.

When the FTC was first created, the primary goal was to prevent unfair methods of competition. At that time, there were many special trusts in existence. These trusts were often engaged in anticompetitive practices, such as:

- Business monopolies
- Restraining trade
- Fixing prices

The creation of the FTC was one of many steps taken to "bust the trusts." Over the years, Congress has passed several consumer protection laws that the FTC enforces. These laws grant the FTC authority to address consumer protection and unfair competition issues.

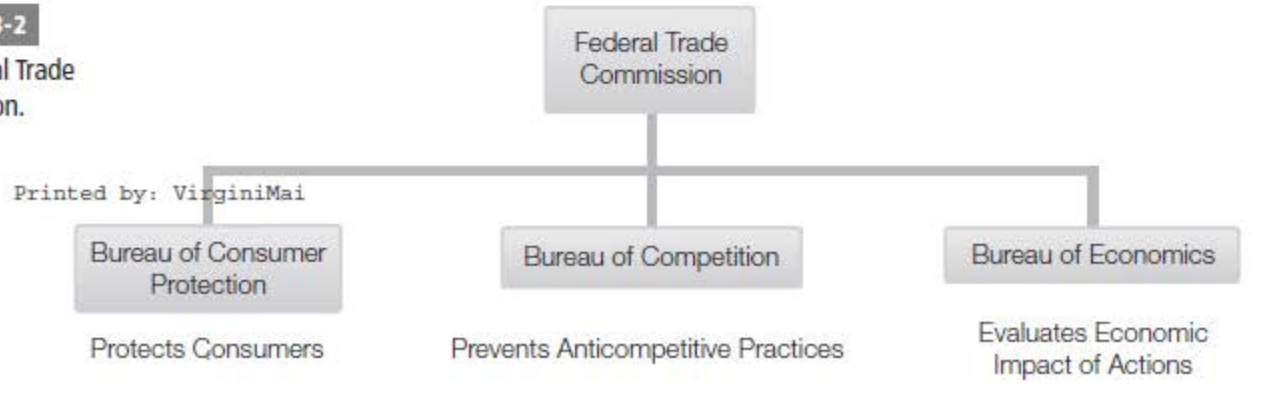
At this point, the original trusts are gone. However, the FTC is still in existence and the focus has shifted to promote consumer protection.

Figure 3-2 shows the hierarchy of the FTC. As indicated in the figure, the FTC has three primary bureaus. These bureaus perform the following actions:

- **Bureau of Consumer Protection**—This bureau tries to protect consumers against unfair, deceptive, or fraudulent practices. The bureau enforces many consumer protection laws and trade regulation rules.
- **Bureau of Competition**—This bureau is the FTC's antitrust arm. It seeks to prevent anticompetitive actions. These actions include anticompetitive mergers and anticompetitive business practices.
- **Bureau of Economics**—This bureau helps the FTC evaluate the economic impact of FTC actions. It provides economic analysis for different investigations. It also evaluates the economic impact of government regulations.

The FTC also has several supporting offices that perform additional work in support of the FTC.

FIGURE 3-2
The Federal Trade Commission.



State Attorney General

Every state has a state **Attorney General (AG)**. The AG is the primary legal advisor for the state. For many states, the AG is also the chief law enforcement officer. Although all states have an AG, the specific responsibilities can vary from state to state. For example, in some states the AG is tasked with specific IT issues, such as preventing identity theft.

The following are some of the responsibilities that can be assigned to an AG:

- Representing the state in all legal matters
- Defending the laws of the state
- Providing legal advice to all state entities
- Performing criminal investigations and prosecuting crimes as the chief law enforcement officer
- Reviewing all deeds, leases, and contracts for the state
- Protecting consumers by fighting identity theft and online scams
- Proposing legislation

Some AGs are elected. Others are appointed by the governor or other state officials.

U.S. Attorney General

The **U.S. Attorney General (U.S. AG)** is the head of the United States Department of Justice (DOJ). The president of the United States nominates the U.S. AG.

Specific responsibilities of the DOJ include:

- Enforcing the law
- Defending the interests of the United States according to the law
- Ensuring public safety against threats
- Providing federal leadership in preventing and controlling crime
- Seeking just punishment for those guilty of unlawful behavior
- Ensuring fair and impartial justice for all Americans

Power of Attorney

A power of attorney can be given to any individual to grant certain rights. For example, you can give a friend a power of attorney to sell your car in your absence. She can then legally act for you in the sale of the car.

It's also possible to grant a general power of attorney. A general power of attorney allows one person to act for another for any legal issues. A general power of attorney is sometimes used if someone becomes mentally incapacitated.

A state AG is a person who is granted the authority to represent the state in all legal matters. This is similar to how a general power of attorney is used. You can think of a state AG as a person granted a general power of attorney for the state.

FYI

Intellectual property (IP) is any intangible property that is the result of creativity and is produced by a person or company. Specific rights are granted to the owner of the creation. This includes music, programs, books, movies, trademarks, trade secrets, and more. The creator and owner should be able to reap the profits from the creation. However, when intellectual property rights are ignored, others benefit at the expense of the creator.

Many actions that the U.S. AG takes fall into the arena of IT. For example, the U.S. AG announced an intellectual property task force in February 2010. Companies, organizations, and governments often transfer data using intellectual property systems and networks. The goal is to address intellectual property crimes on the national and international level. Many government leaders agree that the theft of intellectual property does significant harm to the economy.

Organizational Policies for Compliance

Organizations often implement policies to ensure they remain compliant with different laws and regulations. These policies can contain multiple elements. However, in the context of this chapter, the most important element is **fiduciary responsibility**.

Fiduciary refers to a relationship of trust. A fiduciary could be a person who is trusted to hold someone else's assets. The trusted person has the responsibility to act in the other person's best interests. He or she should avoid conflicts of interest.

Once someone trusts a fiduciary, a fiduciary relationship exists. Notice that this requires two separate entities. The fiduciary responsibility can take many forms. Some examples of fiduciary responsibilities are:

- **An attorney and a client**—The client trusts the attorney to act in the best interests of the client.
- **A CEO and a board of directors**—The board trusts the CEO to act in the best interests of the company.
- **Shareholders and a board of directors**—Shareholders trust the board to act in the best interests of the shareholders.

A great deal of trust is granted in a fiduciary relationship. Because of this, the fiduciary is expected to take extra steps to uphold this trust. Two steps that can be taken are **due diligence** and **due care**:

- **Due diligence**—The fiduciary takes a reasonable amount of time and effort to identify risks. They investigate risks so they are understood. Failure to exercise due diligence can be considered negligence.
- **Due care**—If a risk is known, the fiduciary needs to take reasonable steps to protect against the risks. Failure to take due care to protect assets can also be considered negligence.

Exercising due care and due diligence doesn't mean that all risks should be eliminated. Residual risk is the amount of risk that remains after controls have been applied. It's also referred to as acceptable risk.

A fiduciary is expected to understand and weigh the risks. By exercising due care and due diligence, the fiduciary is less likely to be accused of acting recklessly or being negligent.

Other elements of an organizational policy could include:

- **Mandatory vacations**—Employees may be required to take an annual vacation of at least five consecutive days. The purpose of a **mandatory vacation** is to reduce fraud or embezzlement. If an employee is required to be out of the office, someone else must perform the duties. This increases the likelihood of discovering the illegal activities.
- **Job rotation**—Employees may be rotated through different jobs. When an employee is transferred into a new job, past transactions are often reviewed and examined. This oversight can uncover suspicious activity. **Job rotation** helps prevent or reduce fraudulent activity. Job rotation is also done for cross-training to expand the skills of employees.
- **Separation of duties**—This ensures that no single person controls an entire process. It helps prevent fraud, theft, and errors. Separation of duties also prevents conflicts of interest.
- **Acceptable use**—An **acceptable use policy (AUP)** defines acceptable use for IT systems and data. Companies often inform employees of acceptable use when they are hired. Companies also sometimes use banners and logon screens to remind personnel of the policy.

Standards and Guidelines for Compliance

Several standards and guidelines exist that can be used to assess and improve security. Most of these standards are optional. However, some are mandatory for certain sectors. For example, the PCI DSS is required for merchants using specific credit cards.

The standards and guidelines covered in this section include:

- Payment Card Industry Data Security Standard (PCI DSS)
- National Institute of Standards and Technology (NIST)
- Generally Accepted Information Security Principles (GAISP)
- Control Objectives for Information and related Technology (COBIT)
- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)
- Information Technology Infrastructure Library (ITIL)
- Capability Maturity Model Integration (CMMI)
- Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP)

Payment Card Industry Data Security Standard

The **Payment Card Industry Data Security Standard (PCI DSS)** is an international security standard. The purpose is to enhance security of credit card data. It was created by the PCI Security Standards Council with input from several major credit card companies. These companies include:

- American Express
- Discover Financial Services
- JCB International
- MasterCard Worldwide
- Visa Inc. International

The goal is to thwart theft of credit card data. Fraud can occur if a thief gets certain data. The key pieces of data are:

- Name
- Credit card number
- Expiration date
- Security code

Theft becomes easy if a thief has all of this information.

This data is often transmitted to and from the merchant. It can travel wirelessly from point-of-sale machines. It travels from the merchant's computer to an approval authority. It can be intercepted any time it's transmitted. It can be easily read if it is not encrypted.

For example, data from as many as 100 million credit cards was intercepted from a large retail chain between July 2005 and December 2006. Losses on Visa cards alone were close to $83 million. Millions of customers sued the retailer. The banks that issued the cards also sued the retailer. All of these problems could have been prevented with some basic security.

The PCI DSS is built around six principles. Each of these principles has one or two requirements. The principles and requirements are:

- **Build and Maintain a Secure Network**
  Requirement 1: Install and maintain a firewall.
  Requirement 2: Do not use defaults, such as default passwords.
- **Protect Cardholder Data**
  Requirement 3: Protect stored data.
  Requirement 4: Encrypt transmissions.
- **Maintain a Vulnerability Management Program**
  Requirement 5: Use and update antivirus software.
  Requirement 6: Develop and maintain secure systems.
- **Implement Strong Access Control Measures**
  Requirement 7: Restrict access to data.
  Requirement 8: Use unique logons for each user. Don't share usernames and passwords.
  Requirement 9: Restrict physical access.

Credit Card Data Risky Behavior

The PCI Security Standards Council reports that many organizations take needless risks with credit card data. When an organization stores credit card data, it can be stolen. However, the data often does not need to be stored.

Consider a credit card transaction at a retailer. The retailer needs the name, card number, and expiration date. It sends these for approval. The retailer only needs to keep the amount of the charge and an approval number. It can discard the other data. However, if it keeps all the data, this becomes a risk.

In 2007, Forrester Consulting was commissioned by RSA to conduct a PCI compliance survey of businesses in the United States and Europe. The survey found:

- 81 percent store credit card numbers.
- 73 percent store card expiration dates.
- 71 percent store card verification codes.
- 57 percent store data from the card's magnetic stripe.
- 16 percent store other personal data.

According to the Privacy Rights Clearinghouse, more than 234 million records have been breached since 2005. This sensitive data can be used to steal identities. It can also be used to fraudulently use credit cards.

On the other hand, if this data is not stored, the business is not at risk. Many merchants don't need to store the information. They can capture the data for a single transaction. When the transaction is complete, they can destroy the data.

- **Regularly Monitor and Test Networks**
  Requirement 10: Track and monitor all access to systems and data.
  Requirement 11: Regularly test security.
- **Maintain an Information Security Policy**
  Requirement 12: Maintain a security policy.

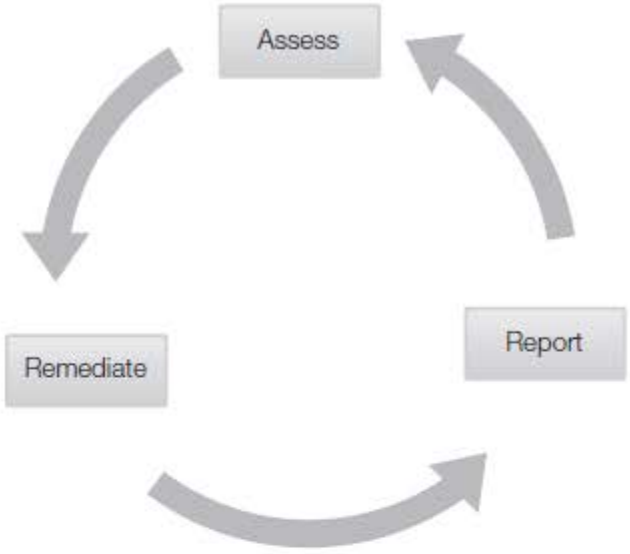
Merchants using credit cards are required to comply with PCI DSS. Compliance is monitored by the acquirer. This is the company that authenticates the transactions.

Compliance with PCI DSS is a three-step continuous process. This process is shown in Figure 3-3:

- **Assess**—The merchant inventories IT assets and processes used for credit card data. It identifies existing cardholder data. It then analyzes data and processes for vulnerabilities.
- **Remediate**—The merchant corrects vulnerabilities. It stores data only when necessary.
- **Report**—The merchant submits compliance reports to the acquiring banks.

This process is repeated at different times.

FIGURE 3-3
PCI compliance process.



Although PCI DSS compliance helps prevent losses, it isn't foolproof. For example, attackers stole credit card data on 40 million customers in a major attack against Target Corporation in late 2013. Attackers also stole personal information on up to 70 million more customers in the same attack. Target was certified as PCI DSS compliant during the attack. The same attack compromised 1.1 million cards at Neiman Marcus. Michael Kingston, CIO at Neiman Marcus, stated that the company's security measures exceeded PCI standards.

A PCI DSS investigation might reveal a problem missed by the PCI DSS assessments that certified these companies. In the past, PCI DSS has retroactively revoked PCI compliance. This allows them to state "no PCI compliant organization has ever been breached." However, many

and Test Networks

National Insti ack and monitor all access to systems and data.
Requirement 11: Regularly test security.

- **Maintain an Information Security Policy**
  Requirement 12: Maintain a security policy.

Merchants using credit cards are required to comply with PCI DSS. Compliance is monitored by the acquirer. This is the company that authenticates the transactions.

Compliance with PCI DSS is a three-step continuous process. This process is shown in Figure 3-3:

- **Assess**—The merchant inventories IT assets and processes used for credit card data. It identifies existing cardholder data. It then analyzes data and processes for vulnerabilities.
- **Remediate**—The merchant corrects vulnerabilities. It stores data only when necessary.
- **Report**—The merchant submits compliance reports to the acquiring banks.

This process is repeated at different times.

- **The Process**—This chapter describes the process of risk assessments. It includes information on how to prepare for and how to conduct the assessment. It also provides detailed information on how to perform six key risk assessment tasks. The tasks are:
  - Identify relevant threat sources.
  - Identify potential threat events related to the threat sources.
  - Identify vulnerabilities threats can exploit.
  - Determine the likelihood threats will occur and can succeed.
  - Determine the adverse impact if a threat exploits a vulnerability.
  - Determine the risk by combining the likelihood and impact.

Generally Accepted Information Security Principles

The Generally Accepted Information Security Principles (GAISP) is an older standard. It evolved from Generally Accepted System Security Principles (GASSP). GASSP was created in 1992. GAISP was an update to GASSP.

GAISP version 3 was released in August 2003. It was adopted by the Information Systems Security Association (ISSA). However, GAISP is no longer mentioned on the ISSA Web site. Additionally, the gaisp.org Web site is no longer maintained.

> **NOTE**
> GASSP and GAISP are no longer active. You may still see them mentioned in some documentation.

GAISP includes two major sections:

- **Pervasive principles**—These principles provide general guidance. The goal is to establish and maintain information security.
- **Broad functional principles**—These principles are derived from the pervasive principles. They represent broad goals of information security (IS).

Control Objectives for Information and Related Technology

Control Objectives for Information and related Technology (COBIT) is a set of good practices. It applies to IT management and IT governance. **IT governance (ITG)** refers to the processes that ensure IT resources are enabling the organization to achieve its goals. Further, ITG processes help ensure the effectiveness and efficiency of these resources. COBIT helps link business goals with IT gone Information Technology Laboratory (ITL). The ITL develops standards

The IT Governance Inrelated to IT. They are published as special publications whose titles have previously known as theP 800-30, "Guide for Conducting Risk Assessments," is valuable when studying risk management.

SP 800-30 includes three chapters:

- **Introduction**—This short chapter identifies the objectives and gives some references.
- **The Fundamentals**—This chapter discusses the importance of risk assessment. It includes definitions for many key risk terms. It also presents some models used to assess risk.

The five principles are:

- **Meeting stakeholder needs**—A stakeholder is any entity affected by activity. In this case, stakeholders are typically decision makers who benefit from IT resources.
- **Covering the enterprise end-to-end**—All areas of responsibility are included.
- **Applying a single integrated framework**—COBIT 5 uses a single integrated framework. This avoids conflicts when using multiple frameworks.
- **Enabling a holistic approach**—This ensures the organization is examined as a whole.
- **Separating governance from management**—Governance includes evaluating, directing, and monitoring. Management includes planning, building, running, and monitoring.

Figure 3-4 shows the seven COBIT enablers. The following bullets describe them:

- **Principles, policies, and frameworks**—These translate desired behavior into practical guidance.
- **Processes**—These are the practices and activities performed within the organization. Processes help an organization reach its IT-related goals.
- **Organizational structures**—This refers to the entities making key decisions.
longer maintained.
- des two major sections:

principles—These principles provide general guidance. The goal is to establish and maintain information security.

- **Broad functional principles**—These principles are derived from the pervasive principles. They represent broad goals of information security (IS).

Control Objectives for Information and Related Technology

Control Objectives for Information and related Technology (COBIT) is a set of good practices. It applies to IT management and IT governance. **IT governance (ITG)** refers to the processes that ensure IT resources are enabling the organization to achieve its goals. Further, ITG processes help ensure the effectiveness and efficiency of these resources. COBIT helps link business goals with IT goals.

The IT Governance Institute (ITGI) worked with ISACA to develop COBIT. ISACA was previously known as the Information Systems Audit and Control Association. However, it now uses only the acronym. You can access many of the free COBIT resources from ISACA's Web site at *http://www.isaca.org/cobit/pages/default.aspx*.

ISACA published COBIT 5 in 2012. Some organizations still use COBIT 4.1. COBIT 5 consolidated COBIT 4.1 and added additional frameworks.

The overall goal of COBIT 5 is to get the most value from IT assets. Organizations do this by maintaining a balance between benefits, risk, and asset use. COBIT 5 is based on five principles and seven enablers. These are generic enough that organizations of any size can apply them.

International Organization for Standardization

The **International Organization for Standardization (ISO)** develops and publishes standards. It includes members from 164 countries. The main office is in Geneva, Switzerland.

ISO works with the International Electrotechnical Commission (IEC). Many of the standards are published as ISO/IEC standards. However, it's common to see the standards abbreviated as ISO. For example, the ISO/IEC 27002 standard is frequently shortened to ISO 27002.

ISO has published many standards that are relevant to risk and IT. Three important standards are:

- ISO 27002 Security Techniques
- ISO 31000 Principles and Guidelines on Implementation
- ISO 73 Risk Management—Vocabulary

You can purchase documentation for these standards from the *http://www.iso.org* Web site.

ISO 27002 Information Technology Security Techniques

ISO 27002 is a set of guidelines and principles. These are used for security management. The current version is ISO 27002:2013. It was derived from the British Standard (BS) 7799. It is a well-respected standard.

The ISO number has been changing over the years. The following list shows the history:

- **ISO/IEC 17799:2000**—The first ISO version of this document.
- **ISO/IEC 17799:2005**—An update to ISO/IEC 17799:2000.
- **ISO/IEC 17799:2005/Cor 1: 2007**—This is a one-correction document.
- **ISO/IEC 27002:2005**—This includes ISO/IEC 17799:2005 and ISO/IEC 17799:2005/Cor 1: 2007. The content is identical to 17799 but the number is changed to 27002.
- **ISO/IEC 27002:2013**—This was published as a major update. However, most of the changes just moved and renumbered content.

You can identify an organization as ISO 27002 certified. Certification requires a two-step process. First, the organization must implement certain best practices. Second, an outside source must evaluate the practices.

These best practices are related to:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Access control
- Incident management
- Business continuity
- Compliance

ISO 31000 Risk Management Principles and Guidelines

ISO 31000:2009 provides generic guidance on risk management. It is not specific to any specific industry or sector. In other words, it doesn't apply only to IT.

An organization can use the principles and guidelines throughout its life. It can apply them to any type of risk.

There is no certification process for ISO 31000. For comparison, an organization can become ISO 27002 certified. There's no such thing as ISO 31000 certified.

Two supplementary documents associated with ISO 31000 are:

- ISO 73 Risk Management—Vocabulary
- IEC 31010 Risk Management—Risk Assessment Techniques

NOTE

The ISO 73:2009 standard replaced the ISO/IEC 73:2002 document.

ISO 73 Risk Management—Vocabulary

ISO 73:2009 is a list of terms. These terms are related to risk management. The goal is to provide a common definition for terms used in risk management.

Definitions can be used by:

- Anyone managing risks

7799. It is a well-respected standard.

The ISO number has been changing over the years. The following list shows the history:

- **ISO/IEC 17799:2000**—The first ISO version of this document.
- **ISO/IEC 17799:2005**—An update to ISO/IEC 17799:2000.
- **ISO/IEC 17799:2005/Cor 1: 2007**—This is a one-correction document.
- **ISO/IEC 27002:2005**—This includes ISO/IEC 17799:2005 and ISO/IEC 17799:2005/Cor 1: 2007. The content is identical to 17799 but the number is changed to 27002.
- **ISO/IEC 27002:2013**—This was published as a major update. However, most of the changes just moved and renumbered content.

You can identify an organization as ISO 27002 certified. Certification requires a two-step process. First, the organization must implement certain best practices. Second, an outside source must evaluate the practices.

These best practices are related to:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Access control
- Incident management
- Business continuity
- Compliance

Information Technology Infrastructure Library

The **Information Technology Infrastructure Library (ITIL)** is a group of books developed by the United Kingdom's Office of Government Commerce (OGC). ITIL has been around since the 1980s and has improved and matured since then. The OGC released ITIL 2011 in July 2011. It replaces ITIL 2007, which was previously called ITIL v3. The differences between ITIL 2007 and ITIL 2011 are minor. Instead, the books have been updated for clarity.

The UK recognized that some companies that were using IT were succeeding. Other companies using similar technologies were failing. One of the goals of ITIL was to document the differences. Early versions of ITIL identified best practices. These were proven activities or processes that were successful in many organizations.

ITIL later renamed "best practice" to"good practice." A good practice is a proven, generally accepted practice. It isn't required in every organization. However, good practices are implemented whenever possible. ITIL recommends the use of several frameworks as good practices. Two of the frameworks recommend by ITIL are:

- Control Objectives for Information and related Technology (COBIT), mentioned earlier in this section
- Capability Maturity Model Integration (CMMI), mentioned later in this section

ITIL 2011 is a collection of five books published by the United Kingdom's Office of Government Commerce (OGC). The books focus on the ITIL lifecycle.

The five books are:

- **ITIL Service Strategy**—The Service Strategy book helps an organization identify the services it should provide.
- **ITIL Service Design**—The Service Design book details how identified services can be implemented.
- **ITIL Service Transition**—The Service Transition book focuses on introducing the services. This also includes modifying or changing services. Most companies have learned the hard way that if changes aren't managed, changes can take systems down. Change management has become very important for many companies.

NOTE

One of the drawbacks to ITIL is the availability of materials. The five ITIL books have a retail cost of about $549.

FYI

ITIL is centered on services. A service is a means of delivering value to customers. It gives customers what they want. It doesn't require the customer to take ownership of the costs and risks. For example, e-mail is a service. Customers want to be able to send and receive e-mail. Most customers don't want to own and manage the e-mail servers. In this context, e-mail can be provided to employees from the IT department. The employees are the customers. The IT department is the service provider.

- **ITIL Service Operation**—The Service Operation book focuses on day-to-day operations.
- **ITIL Continual Service Improvement**—The Continual Service Improvement book focuses on methodologies used to improve the services.

Figure 3-5 shows the relationships between the five phases of the ITIL lifecycle. Any service implemented and managed within an IT organization will go through several phases. There are different concerns and requirements at each phase.

For example, consider e-mail as a provided service. Imagine that your company was moving from outsourced e-mail to an internal e-mail server. The company could use the ITIL lifecycle for each phase of the implementation:

- **Service Strategy phase**—You evaluate services to determine if they have value to the organization. E-mail could provide value with improved sales. It could provide improved productivity due to better communication. If you determine that internal e-mail will provide value, the process continues to the next phase.
- **Service Design phase**—IT designs services for use within the organization. In this phase, you'd design your e-mail solution. For example, your IT network may be a Microsoft Windows domain, so you would design a Microsoft Exchange solution. You would identify how many servers to add and any changes needed in the network to support them.
- **Service Transition phase**—This phase includes adding and modifying services. It also includes removing obsolete services. A primary goal of this phase is to ensure the transition does not cause an outage. Adding a Microsoft Exchange e-mail solution, for example, would include several elements. You would need to modify the Active Directory schema. You may need to add global catalog servers. You would build Microsoft Exchange servers. You would install applications on user computers. You would provide training to everyone from end users to technicians maintaining the new servers.
- **Service Operation phase**—Daily operations and support of any service is handled here. For e-mail, this can include regular maintenance and handling any incidents that impact the service. It would also include performing backups and test restores. The goal here is to ensure the end users have access to their e-mail when they expect to have it.
- **Continual Service Improvement phase**—This phase focuses on measuring and monitoring services and processes. The goal is to determine areas where services can be improved. This can include regular monitoring and performance tuning of the e-mail servers. You can use analysis to identify problem areas before they become actual problems. This can provide insight into areas that can be improved.

You can access ITIL resources at *http://www.itil-officialsite.com/*.

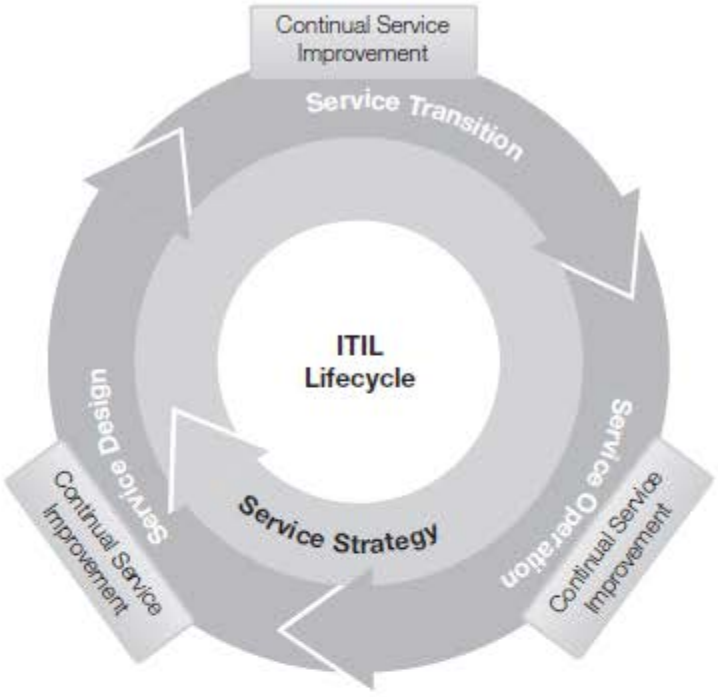


FIGURE 3-5
ITIL lifecycle.

ITIL Certifications

More and more organizations are recognizing the value of ITIL. They are requiring IT personnel to learn and adopt ITIL practices. Just as you would want certified health care professionals to treat you, many organizations want to ensure a certain percentage of IT employees are certified in ITIL.

ITIL certifications validate knowledge at different levels. The first level is ITIL Foundation. IT administrators and IT managers often pursue this.

From there, you can specialize in different areas of ITIL. The highest level is ITIL Master Qualification.

Global Knowledge did a salary survey in 2013. ITIL certs were listed in the top salary ranges. Individuals with the basic ITIL Foundation certificate earned almost $100,000. In some areas of the United States, they earned about $92,000.

It should be noted that most people with ITIL certs have other skills. ITIL practitioners start with a solid foundation in IT. That path may lead them to be IT administrators or managers for IT teams. The ITIL knowledge helps them ensure the IT network works as smoothly as possible.

Capability Maturity Model Integration

The **Capability Maturity Model Integration (CMMI)** is a process improvement approach to management. It uses different levels to determine the maturity of a process.

CMMI can be used in three primary areas of interest:

- **Product and service development**—CMMI is often used with software development. It helps ensure the final product meets the original goals. It also helps ensure the product is completed within budget and time constraints.
- **Service establishment, management, and delivery**—CMMI can be used to measure the effectiveness of services. Security can be considered a service. Security helps ensure confidentiality, integrity, and availability of data and systems.
- **Product and service acquisition**—This can be used to ensure you consistently buy what you need. It also helps to ensure you get what you pay for.

Figure 3-6 shows the six levels of the CMMI. These are also referred to as CMMI characteristics.

You can use these levels to determine the effectiveness of security within an organization. The following list identifies the levels and how they can be used to evaluate security. Although Level 0 is listed here, it is sometimes omitted:

- **Level 0: Nonexistent**—Security controls are not in place. There is no recognition of a need for security.
- **Level 1: Initial**—This is sometimes referred to as ad hoc, or as needed. Risks are considered after a threat exploits a vulnerability.

FIGURE 3-6
CMMI characteristics.

- **Level 2: Managed**—The organization recognizes risks. The organization recognizes a need for security. However, it performs controls out of intuition rather than from detailed plans. Responses are reactive.
- **Level 3: Defined**—The organization has security policies in place. It has some security awareness. Action is proactive.
- **Level 4: Quantitatively Managed**—The organization measures and controls security processes. It has formal policies and standards in place. It performs regular risk assessments and vulnerability assessments.
- **Level 5: Optimized**—The organization has formal security processes in place throughout the organization. It monitors security on a continuous basis. Its focus is on process improvement.

Level 5 shows the highest level of maturity.

Department of Defense Information Assurance Certification and Accreditation Process

The **Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP)** is a risk management process. DIACAP is used for IT systems used by the U.S. DoD. It is fully documented in DoD instruction 8510.1.

DIACAP details specific phases that IT systems must go through. The core goal is to ensure systems are in compliance with requirements. These phases are:

- **Phase 1: Initiate and Plan**—Register the system with DIACAP. Assign information assurance (IA) controls. Create a DIACAP team. Develop a DIACAP strategy. Begin the IA plan.
- **Phase 2: Implement and Validate**—Implement the IA plan. Update the IA plan if needed. Validation activities verify compliance of the system. Document validation results.
- **Phase 3: Make Certification and Accreditation Decisions**—Analyze residual risk. Review documentation to verify certification. A decision is made to accredit the system. Once the system is accredited, it receives an authorization to operate (ATO).
- **Phase 4: Maintain ATO/Review**—Maintain the system. The goal is to ensure it stays in compliance with the requirements of the ATO. Periodically review the system for compliance.
- **Phase 5: Decommission**—Decommission the system. Dispose of DIACAP data.

> **NOTE**
> DIACAP replaced DITSCAP in 2007. DITSCAP was an acronym for DoD Information Technology Security Certification and Accreditation Process.

NOTE

(ISC)² sponsors several certifications. The Systems Security Certified Practitioner (SSCP) is one security certification. The Certified Information Systems Security Professional (CISSP) is a higher-level certification.

(ISC)² offers a civilian-based certification that you can use for DoD 8570.1. It is called Certification and Accreditation Professional (CAP). It requires two years' experience in the certification and accreditation field. You must also pass an exam with a score of at least 700.

CHAPTER SUMMARY

IT systems and data need to be protected. For the organizations that won't do this on their own, there are now many laws in place. Many of these laws are designed to ensure that the IT systems and data are protected.

Beyond the laws, there are also many regulations that apply to specific sectors. Additionally, there is a wide assortment of standards and guidelines related to IT. Many of these can be used by any organization to help it assess and improve its own security.

KEY CONCEPTS AND TERMS

Acceptable use policy (AUP)
Attorney General (AG)
Capability Maturity Model Integration (CMMI)
Children's Internet Protection Act (CIPA)
Compliance
Control Objectives for Information and related Technology (COBIT)
Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP)
Due care
Due diligence
Family Educational Rights and Privacy Act (FERPA)
Federal Deposit Insurance Corporation (FDIC)
Federal Information Security Management Act (FISMA)
Federal Trade Commission (FTC)
Fiduciary responsibility
Gramm-Leach-Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA)
Information Technology Infrastructure Library (ITIL)
Intellectual property (IP)
International Electrotechnical Commission (IEC)
International Organization for Standardization (ISO)
IT governance (ITG)
Job rotation
Mandatory vacation
Payment Card Industry Data Security Standard (PCI DSS)
Sarbanes-Oxley Act (SOX)
Securities and Exchange Commission (SEC)
U.S. Attorney General (U.S. AG)

CHAPTER 3 ASSESSMENT

1. FISMA requires federal agencies to protect IT systems and data. How often should compliance be audited by an external organization?

A. Never
B. Quarterly
C. Annually
D. Every three years

2. What law applies to organizations handling health care information?

A. SOX
B. GLBA
C. FISMA
D. HIPAA

3. CEOs and CFOs can go to jail if financial statements are inaccurate. What law is this from?

A. SOX
B. GLBA
C. FISMA
D. HIPAA

4. What law requires schools and libraries to limit offensive content on their computers?

A. FERPA
B. HIPAA
C. CIPA
D. SSCP

5. Employees in some companies are often required to take an annual vacation of at least five consecutive days. The purpose is to reduce fraud and embezzlement. What is this called?

A. Job rotation
B. Mandatory vacation
C. Separation of duties
D. Due diligence

6. Fiduciary refers to a relationship of trust.

A. True
B. False

7. Merchants that handle credit cards are expected to implement data security. What standard should they follow?
   A. GAISP
   B. CMMI
   C. COBIT
   D. PCI DSS

8. The National Institute of Standards and Technology published Special Publication 800-30. What does this cover?
   A. Risk assessments
   B. Maturity levels
   C. A framework of good practices
   D. Certification and accreditation

9. The COBIT framework refers to IT governance. Of the following choices, what *best* describes IT governance?
   A. IT-related laws
   B. IT-related regulations
   C. Processes to manage IT resources
   D. Processes to manage IT-related laws and regulations

10. This standard is focused on maintaining a balance between benefits, risk, and asset use. It is based on five principles and seven enablers. What is this standard?
    A. COBIT
    B. ITIL
    C. GAISP
    D. CMMI

health care information?
   A. SOX
   B. GLBA
   C. FISMA
   D. HIPAA

3. CEOs and CFOs can go to jail if financial statements are inaccurate. What law is this from?
   A. SOX
   B. GLBA
   C. FISMA
   D. HIPAA

11. Which of the following ISO standards can be used to verify that an organization meets certain requirements? Part I identifies objectives and controls. Part II is used for certification.
    A. ISO 73 Risk Management—Vocabulary
    B. ISO 27002 Information Technology Security Techniques
    C. ISO 31000 Risk Management Principles and Guidelines
    D. IEC 31010 Risk Management—Risk Assessment Techniques

12. Which of the following ISO documents provides generic guidance on risk management?
    A. ISO 73 Risk Management—Vocabulary
    B. ISO 27002 Information Technology Security Techniques
    C. ISO 31000 Risk Management Principles and Guidelines
    D. IEC 31010 Risk Management—Risk Assessment Techniques

13. ITIL is a group of five books developed by the United Kingdom's Office of Government Commerce.
    A. True
    B. False

14. In the CMMI, level _____ indicates the highest level of maturity.

15. The DIACAP is a risk management process applied to IT systems. What happens after

5. Employees in some companies are often required to take an annual vacation of at least five consecutive days. The purpose is to reduce fraud and embezzlement. What is this called?
   A. Job rotation
   B. Mandatory vacation
   C. Separation of duties
   D. Due diligence

6. Fiduciary refers to a relationship of trust.
   A. True
   B. False

Developing a Risk Management Plan

CHAPTER 4

A RISK MANAGEMENT PLAN is a specialized type of project management. You apply many of the same techniques to risk management that you would when managing any project. At the core is the need to plan. As the old saying goes, if you fail to plan, you plan to fail. Without a risk management plan, failure is much more likely than success.

A well-documented risk management plan helps ensure you are able to reach your desired goal. Primarily, you create a risk management plan to mitigate risks. This plan helps you identify the risks and choose the best solutions. It also helps you track the solutions to ensure they are implemented on budget and on schedule. A fully implemented plan will include a plan of action and milestones (POAM). You can then use the POAM to track the project.

Chapter 4 Topics

This chapter covers the following topics and concepts:

- What the objectives of a risk management plan are
- What the scope of a risk management plan is
- How to assign responsibilities in a risk management plan
- How procedures and schedules are described in the risk management plan
- What the reporting requirements are
- What a plan of action and milestones is
- How to chart the progress of a risk management plan

Chapter 4 Goals

When you complete this chapter, you will be able to:

- Describe the objectives of a risk management plan
- Describe the purpose of a plan's scope
- Identify the importance of assigning responsibilities
- Describe the purpose of the procedures list in a risk management plan
- List reporting requirements of a risk management plan
- Document findings of a risk management plan
- Create a plan of action and milestones
- Identify a milestone plan chart
- Identify a Gantt chart and define a critical path chart

Objectives of a Risk Management Plan

One of the important first steps for a risk management plan is to establish the objectives. The objectives become the road map for your plan. They help you identify where you're going and, just as important, they help you know when you've arrived. You should establish objectives for the plan as early as possible.

The objectives identify the goals of the project. These objectives outline what you should include in the plan. Some common objectives for a risk management plan are:

- A list of threats
- A list of vulnerabilities
- Costs associated with risks
- A list of recommendations to reduce the risks
- Costs associated with recommendations
- A cost-benefit analysis
- One or more reports

While the reports document the above items, the risk management plan doesn't end there. Once top managers receive a report, they will be able to make decisions based on the data. They will accept some recommendations. They may modify some. And they may defer some.

The next phase of the risk management plan covers implementation of the plan. Implementation involves the following tasks:

- Document management decisions.
- Document and track implementation of accepted recommendations.
- Include a POAM.

Throughout this chapter, two examples are used. These examples show how you can create a risk management plan for actual projects. The two examples are:

- **Web site**—Your company, Acme Widgets, hosts a Web site used to sell widgets on the Internet. The Web site is hosted on a Web server owned and controlled by your company. The Web site was recently attacked and went down for two days. The company lost a large amount of money. Additionally, the company lost the goodwill of many customers. This was the second major outage for this Web site in the past two months. There have been many outages in the past three years.
- **Health Insurance Portability and Accountability Act (HIPAA) compliance**—Your company recently purchased Mini Acme. Mini Acme has not complied with HIPAA. Management wants to identify the risks associated with this noncompliance. Managers also want to ensure that issues are corrected as soon as possible.

> **NOTE**
> The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 to ensure protection of health information data. Title II of HIPAA covers the protection of health data.

After the chapter covers a topic, these examples are sometimes used to show how you could create a portion of the plan. The examples aren't intended to show the only possible way to create a plan. An actual plan could vary based on the needs of your company.

Objectives Example: Web Site

The Acme Widgets Web site has suffered outages. These outages resulted in unacceptable losses. The losses could have been prevented by managing Web site risks. You can use the risk management plan to identify these risks.

The objectives of the plan are to:

- **Identify threats**—This means any threats that directly affect the Web site. These may include:
  - Attacks from the Internet
  - Hardware or software failures
  - Loss of Internet connectivity
- **Identify vulnerabilities**—These are weaknesses and may include:
  - Lack of protection from a firewall
  - Lack of protection from an intrusion detection system
  - Lack of antivirus software
  - Lack of updates for the server
  - Lack of updates for the antivirus software

> **NOTE**
> A **firewall** filters traffic. Firewall rules are configured to specifically allow certain traffic. Most firewalls block all traffic that is not specifically allowed. You can use both network and host-based firewalls. A network firewall usually consists of both hardware and software and filters traffic for the network. Individual systems can have a software firewall that filters traffic for a single system.

- **Assign responsibilities**—Assign responsibility to specific departments for collecting data. This data will be used to create recommendations. Later in the plan, you will assign responsibilities to departments to implement and track the plan.
- **Identify the costs of an outage**—Include both direct and indirect costs. The direct costs are the lost sales during the outage. The amount of revenue lost if the server is down for 15 minutes or longer will come from sales data. Indirect costs include the loss of customer goodwill and the cost to recover the goodwill.
- **Provide recommendations**—Include a list of recommendations to mitigate the risks. The recommendations may reduce the weaknesses. They may also reduce the impact of the threats. For example, you could address a hardware failure threat by recommending hardware redundancy. You could address a lack of updates by implementing an update plan.
- **Identify the costs of recommendations**—Identify and list the cost of each recommendation.
- **Provide a cost-benefit analysis (CBA)**—Include a CBA for each recommendation. The CBA will compare the cost of the recommendation against the benefit to the company of implementing the recommendation. You can express the benefit in terms of income gained or the cost of the outage reduced.
- **Document accepted recommendations**—Management will choose which recommendations to implement. They can accept, defer, or modify recommendations. You will then document these choices in the plan.
- **Track implementation**—The plan will track the choices and their implementation.
- **Create a POAM**—Include a POAM that assigns responsibilities. Management will use it to track and follow up on the project.

Objectives Example: HIPAA Compliance

Your company recently acquired Mini Acme. An inspection of some records indicates that health information isn't protected. Your company is therefore not in compliance with HIPAA. Noncompliance can result in fines and jail time.

The purpose of this plan is to ensure compliance with HIPAA. The objectives of the plan are to:

- **Identify threats**—These could be both internal and external threats.
- **Identify vulnerabilities**—These are the weaknesses. They may include:
  - Lack of policies preventing information sharing
  - Lack of protection when the data is stored
  - Lack of protection when the data is transmitted
- **Assign responsibilities**—Assign responsibility to specific departments to identify threats and vulnerabilities. You will use this data to identify corrective actions. Later, you can assign responsibilities to departments to implement and track the plan.

- **Identify the costs of noncompliance**—Costs include the legal fines associated with noncompliance. Additional costs may result from lawsuits or the loss of customer confidence.
- **Provide recommendations**—Create a list of recommendations. This list may include procedural changes. It could include protecting the data with access controls. It could also include encrypting the data during transmissions.
- **Identify the costs of recommendations**—Identify and list the cost of each recommendation.
- **Provide a CBA**—Complete a CBA for each recommendation. It will compare the cost of the recommendation against the cost of the outage.
- **Document accepted recommendations**—Management will choose which recommendations to implement. Managers can accept, defer, or modify recommendations. These choices will be documented in the plan.
- **Track implementation**—The plan will track the choices and their implementation.
- **Create a POAM**—Include a POAM that assigns responsibilities. Management will use it to track and follow up on the project.

Scope of a Risk Management Plan

In addition to the objectives, it's also important to identify the **scope** of a risk management plan. The scope identifies the boundaries of the plan. The boundaries could include the entire organization or a single system. Without defined boundaries, the plan can get out of control.

A common problem with many projects is **scope creep**. Scope creep comes from uncontrolled changes. As the changes creep in, the scope of the project grows. Changes bring in additional requirements. Uncontrolled changes result in cost overruns and missed deadlines.

For example, consider the HIPAA compliance example mentioned earlier. The objective of this project is to bring Mini Acme into compliance with HIPAA. Suppose you find other unprotected data that is not health data. It could be financial data, research data, or user data.

If you roll this data into the project, it would expand the project. You would have to identify threats and vulnerabilities. You would have to calculate the costs of the data loss. You would need to identify additional recommendations and their costs. All of this will take more time and more money.

This is not to say that the scope of a project should never change. The key is to control the changes. A risk management project manager should work with stakeholders to identify what changes are acceptable.

Scope Creep in Application Development

Scope creep is a common problem in application development. Programmers often see how a program can be improved by tweaking it a little here or there. Although the programmers are well intentioned, these changes can sometimes have far-reaching effects.

In one project, a programmer added an additional capability to a program. This change allowed the user to search through data. This was clearly outside the scope of the project. However, it didn't take much time to program it and the change was added without much notice to anyone. The application was then shipped to the customer with the new capability.

The customer used the program successfully for a few months. Later, the format of the data was changed. The change of the format didn't affect the primary purpose of the program. It still worked as required. However, the additional search feature no longer worked.

Who's responsible for fixing the problem? The application developer was responsible.

A change that originally looked like added value actually became added liability. Even though the search capability was outside the scope of the project, it became part of the application. This added capability would have to be maintained just as any other part of the application needs to be maintained. The developer didn't have much choice. If he refused to fix the problem, it would affect the perceived usability of the program.

At this point, it wasn't easy to remove the added capability. It looked and behaved like a feature. While it would not have been missed if it was never added, it would now be missed if it was removed.

NOTE

Companies typically have "C"-level executives identified as CEO, CIO, CFO, and so on. CCO is short for chief compliance officer. CEO is short for chief executive officer. CFO is short for chief financial officer. CIO is short for chief information officer. CSO is short for chief security officer. CTO is short for chief technology officer.

A **stakeholder** is an individual or group that has a stake, or interest, in the success of a project. A key stakeholder is a stakeholder who has authority to make decisions about the project, including the ability to grant additional resources. Examples of a key stakeholder could be a company executive such as a CIO or CFO. It could be a vice president who will "own" the project upon completion.

It's good to involve stakeholders in drafting a scope statement. This involvement can be anything from drafting the statement to approving it. This involvement helps the stakeholder have ownership of the project. Ownership is also referred to as *buy-in* for the project.

A true stakeholder has a vested interest in the project and wants to see it succeed. On the other hand, a stakeholder named as a figurehead without a stake in the project sees it as a nuisance. A project without a true stakeholder will often die due to lack of support. Resources aren't allocated. Decisions aren't made. Team members realize it's not supported and stop contributing.

Consider the unprotected data from the HIPAA example. If a risk management team discovered unprotected financial data, the team could present its concerns to the project manager (PM). The PM can evaluate the data and determine that none of it is HIPAA related but realize it is important. The PM can pass the information on to a stakeholder as an issue of concern. A stakeholder may direct the PM to include the data in the plan. At that point, it is a controlled change.

Sample scope statements for the Web site and HIPAA compliance projects are provided in the following sections.

Scope Example: Web Site

The purpose of the risk management plan is to secure the Acme Widgets Web site. The scope of the plan includes:

- Security of the server hosting the Web site
- Security of the Web site itself
- Availability of the Web site
- Integrity of the Web site's data

Stakeholders for this project include:

- Vice president of sales
- Information technology (IT) support department head

Written approval is required for any activities outside the scope of this plan.

Scope Example: HIPAA Compliance

The purpose of the risk management plan is to ensure compliance with HIPAA for Mini Acme's data. The scope of the plan includes:

- Identification of all health data
- Storage of health data
- Usage of health data
- Transmission of health data

Stakeholders for this project include:

- CIO
- Human resources department head

Written approval is required for any activities outside the scope of this plan.

NOTE

A risk management PM is sometimes called a risk management coordinator. The skills required of a successful risk management PM are the same skills required of a successful project manager for almost any project.

Assigning Responsibilities

The risk management plan specifies responsibilities. This provides accountability. If you don't assign responsibilities, tasks can easily be missed. You can assign responsibilities to:

- The risk management PM
- Stakeholders
- Departments or department heads
- Executive officers such as CIO or CFO

It's important to ensure that any entity that is assigned a responsibility has the authority to complete the task. This is especially important for the PM.

For example, team members may not work directly for the PM. Technicians, say, might work in the IT department. They can be assigned as team members for a project. However, they may still report directly to supervisors in the IT department. So their taskings from the IT department and from the PM may compete with each other. If the PM doesn't have the authority to resolve these problems, it can affect the success of the project. At the very least, the PM should have access to stakeholders to resolve problems.

The PM is responsible for the overall success of the plan. Some of the common tasks of a PM are:

- Ensuring costs are controlled
- Ensuring quality is maintained
- Ensuring the project stays on schedule
- Ensuring the project stays within scope
- Tracking and managing all project issues
- Ensuring information is available to all stakeholders
- Raising issues and problems as they become known
- Ensuring others are aware of their responsibilities and deadlines

Individual responsibilities could be assigned for the following activities:

- **Risk identification**—This includes identifying threats and vulnerabilities. The resulting lists of potential risks can be extensive.
- **Risk assessment**—This means identifying the likelihood and impact of each risk. A threat matrix is a common method used to assess risks.

technical TIP

Consider creating a threat-likelihood-impact matrix. A percentage from 10 percent to 100 percent is assigned for each likelihood. The impact severity is assigned a value between 10 and 100. The value is then calculated by multiplying the two values. Higher values indicate risks that should be addressed first. Lower values indicate risks that may be accepted.

- **Risk mitigation steps**—This means identifying steps that can reduce weaknesses. This can also include steps to reduce the impact of the risk.
- **Reporting**—This means reporting the documentation created by the plan to management. The PM is often responsible for compiling reports.

Examples of responsibility statements for the Web site and HIPAA compliance scenarios are presented in the following two sections.

Responsibilities Example: Web Site

The CFO will provide funding to the IT department to hire a security consultant. This security consultant will assist the IT department.

The IT department is responsible for providing:

- A list of threats
- A list of vulnerabilities
- A list of recommended solutions
- Costs for each of the recommended solutions

The sales department is responsible for providing:

- Direct costs of any outage for 15 minutes or longer
- Indirect costs of any outage for 15 minutes or longer

The CFO will validate the data provided by the IT and sales departments. The CFO will then complete a cost-benefit analysis.

Responsibilities Example: HIPAA Compliance

The human resources (HR) department is responsible for identifying all health information held by Mini Acme. The HR department is responsible for providing:

- A list of all health information sources
- Inspection results for all data sources regarding their compliance with HIPAA:
  - How the data is stored
  - How the data is protected
  - How the data is transmitted
- A list of existing HIPAA policies used by Mini Acme
- A list of needed HIPAA policies
- A list of recommended solutions to ensure compliance with HIPAA
- Costs for each of the recommended solutions
- Costs associated with noncompliance

The IT department is responsible for providing:

- Identification of access controls used for data
- A list of recommended solutions to ensure compliance with HIPAA
- Costs for each of the recommended solutions

Using Affinity Diagrams

While it's easy to assign responsibility, it may not be so easy to identify the tasks. One of the challenges is to generate lists of realistic threats, vulnerabilities, and recommendations. An affinity diagram can help with these tasks.

An **affinity diagram** is created in four basic steps. These are:

- **Identify the problem**—Create a basic problem statement. For example, consider the Web site problem. It could be stated as: "Web site outages result in lost sales."
- **Generate ideas**—The more the better. The ideas can be about any elements of the problem. They can include threats and vulnerabilities. They can also include recommended solutions. **Brainstorming** is one method that can be used. In a brainstorming session, participants are encouraged to mention anything that comes to mind. All ideas are written down without any judgment. The creative process can often bring out a wealth of ideas.
- **Gather ideas into related groups**—After the ideas are generated, group them together. For a risk management plan, the groups will usually fit into categories of threats, vulnerabilities, and recommendations. Some of these categories may include subcategories. For example, you could divide vulnerabilities into network and server weaknesses.
- **Create an affinity diagram**—Figure 4-1 shows an example of an affinity diagram. It groups all of the ideas together.

In an actual scenario, the affinity diagram is likely to be much larger. You could divide threats into external and internal threats. There can be an almost endless list of vulnerabilities.

The CFO will validate the data provided by the IT and sales departments. The CFO will then complete a cost-benefit analysis.

Describing Procedures and Schedules for Accomplishment

You create this part of the risk management plan after the project has started. You include a recommended solution for any threat or vulnerability, with a goal of mitigating the associated risk. While you can summarize a solution in a short phrase, the solution itself will often include multiple steps.

For example, an existing firewall may expose a server to multiple vulnerabilities. The solution could be to upgrade the firewall. This upgrade can be broken down into several steps, such as:

- Determine what traffic should be allowed.
- Create a firewall policy.
- Purchase a firewall.
- Install the firewall.

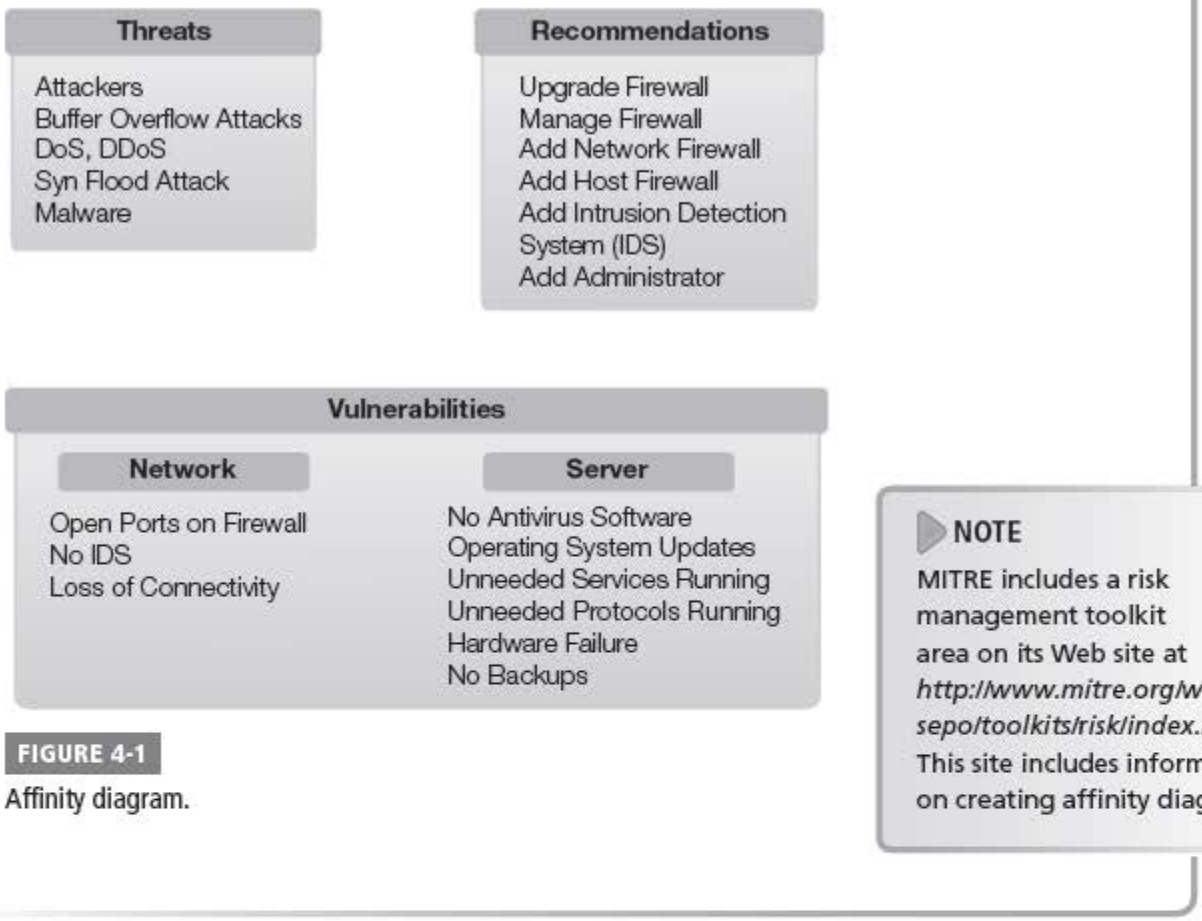


FIGURE 4-1
Affinity diagram.

NOTE

MITRE includes a risk management toolkit area on its Web site at *http://www.mitre.org/work/sepo/toolkits/risk/index.html*. This site includes information on creating affinity diagrams.

- Configure the firewall.
- Test the firewall.
- Implement the firewall.

You can describe each of these steps in further detail. In addition, you can include a timeline for completion of each of the steps.

There are a couple of things to remember at this point:

- Management is responsible for choosing the controls to implement.
- Management is responsible for residual risk.

Because management has not reviewed the recommendations yet, this schedule will usually not include dates. Instead, the schedule will list how long it may take to complete any of the recommendations.

For example, a single recommendation may include five tasks. You can list the time required for each of these tasks. You can add start and end dates later.

Partial listings of procedures for the Web site and HIPAA examples are given in the following sections.

NOTE

A DoS attack is any attack designed to prevent a system from providing a service. A distributed DoS (DDoS) attack is a DoS attack launched from multiple systems at the same time. DDoS attacks often include zombie computers controlled in a botnet.

Procedures Example: Web Site

The Web site is vulnerable to denial of service (DoS) attacks from the Internet. This risk cannot be eliminated. However, several tasks can be completed to mitigate the risk:

- **Recommendation**—Upgrade the firewall.
- **Justification**—The current firewall is a basic router. It filters packets but does not provide any advanced firewall capabilities.
- **Procedures**—The following steps can be used to upgrade the new firewall:

1. Start firewall logging. This log can be used to determine what ports are currently being used. Logs should be collected for at least one week.
2. Create a firewall policy. A **firewall policy** identifies what traffic to allow past the firewall. This is a written document. It is created based on the content of the firewall logs.
3. Purchase a firewall appliance. A **firewall appliance** provides a self-contained firewall solution. It includes both hardware and software that provides protection for a network. Firewall appliances range from $200 to more than $10,000. The SS75 model is recommended at a cost of $4,000. It will arrive within 30 days after ordering.
4. Install the firewall. The firewall could be installed in the server room. Existing space and power are available there.
5. Configure the firewall. Technicians will use the firewall policy to configure the firewall.
6. Test the firewall before going live. Testing will ensure normal operations are not impacted. Technicians can complete testing in one week.
7. Bring the firewall online. Technicians can complete this step within a week after completing tests.

FYI

Firewalls labeled as appliances are intended to be easy to use. The implication is that you can plug them in and they work. You don't have to be an expert in how they work. It's like a toaster. You put bread in and toast comes out. You don't have to know how the toaster works to make toast. Similarly, you don't have to be an expert on firewalls to use a firewall appliance.

Procedures Example: HIPAA Compliance

Employees of Mini Acme are not aware of HIPAA. They don't understand the requirements of the law. They don't understand the consequences of noncompliance. You can complete the following tasks to mitigate the risk of noncompliance:

- **Recommendation**—Increase awareness of HIPAA.
- **Justification**—Make clear that noncompliance can result in fines totaling $25,000 a year for mistakes.
- **Procedures**—Use the following steps to increase awareness:
  1. Require all employees to read and comply with HIPAA policies. Don't create new policies. Require Mini Acme employees to read and acknowledge HIPAA policies currently in place. This can be accomplished in 30 days.
  2. Provide training to all employees on HIPAA compliance. Training will include what data is covered by HIPAA. It will also include consequences of noncompliance. If approved, it will take approximately 60 days to create training materials. Training can be completed in 30 days.

Reporting Requirements

After you collect data on the risks and recommendations, you need to include it in a report. You will then present this report to management. The primary purpose of the report is to allow management to decide on what recommendations to use.

There are four major categories of reporting requirements. They are:

- **Present recommendations**—These are the risk response recommendations.
- **Document management response to recommendations**—Management can accept, modify, or defer any of the recommendations.
- **Document and track implementation of accepted recommendations**—This becomes the actual risk response plan.
- **Create a plan of action and milestones (POAM)**—The POAM tracks the risk response actions.

Presenting Recommendations

You compile the collected data into a report. It will include the lists of threats, vulnerabilities, and recommendations. You then present this report to management. Management will use this data to decide what steps to take.

It's important to remember the overall goal of the risk management plan at this stage. The goal is to identify the risks and recommend strategies to reduce them. Most of the risks won't be eliminated, but instead they will be reduced to an acceptable level. For every risk identified, there will be an accompanying recommendation to reduce the risk.

This report should include the following information:

- Findings
- Recommendation cost and time frame
- Cost-benefit analysis

Findings

The findings list the facts. Remember, losses from risks occur when a threat exploits a vulnerability. Risk management findings need to include threats, vulnerabilities, and potential losses. These are described as cause, criteria, and effect:

- **Cause**—The cause is the threat. For example, an attacker may try to launch a DoS attack. In this case, the threat is the attacker. When you list the cause, it's important to identify the root cause. A successful attack is dependent on an attacker having access and the system being vulnerable. Risk management attempts to reduce the impact of the cause, or reduce the vulnerabilities.
- **Criteria**—This identifies the criteria that will allow the threat to succeed. These are the vulnerabilities. For example, a server will be susceptible to a DoS attack if the following criteria are met:
  - *Inadequate manpower*—If manpower isn't adequate to perform security steps, the site is vulnerable.
  - *Unmanaged firewall*—Each open port represents a vulnerability. If ports are not managed on a firewall, unwanted traffic can be allowed in.
  - *No intrusion detection system (IDS)*—Depending on the type of IDS, it can not only detect intrusions but also respond to intrusions and change the environment.
  - *Operating system not updated*—Apply patches to the system as they are released and tested. If you don't apply updates, the system is vulnerable to new exploits.
  - *Antivirus software not installed and updated*—Antivirus software can detect malware. You should update it with definitions to ensure it will detect new malware.
- **Effect**—The effect is often an outage of some type. For example, the effect on a Web site could be that the Web site is not reachable any more.

An important consideration as you document findings is resource availability. It could be that all the discovered issues were previously known. However, money may not have been allocated to purchase the solutions in the past. It's also possible that manpower wasn't adequate to implement the solutions.

When adequate manpower isn't available, security is often sacrificed for ease of use. Consider the Web site example. The first goal may be to ensure the Web site is operational. Once it's up, resources may be used for other jobs. The Web site may still not be secure, backups may not be made, or other security issues may still exist.

A **cause and effect diagram** can be used to discover and document the findings. Figure 4-2 shows a sample cause and effect diagram for the Web site scenario. In this diagram, the

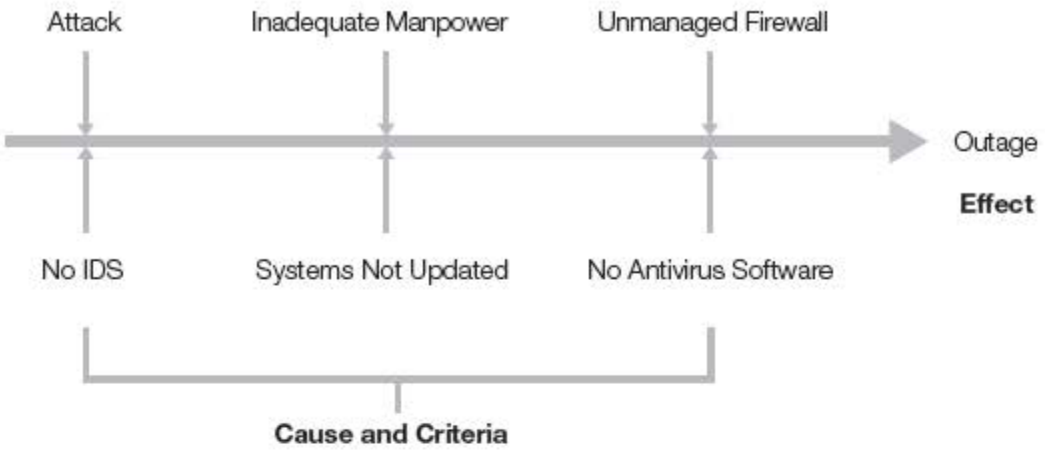


FIGURE 4-2
Web site cause and effect diagram.

primary cause is an attack. The remaining items are contributing factors that allow the attack to succeed. The effect is an outage.

There are several advantages to using a cause and effect diagram. It can help guide discussions during the discovery process. It can also help visualize the relationships between causes and effects in documentation. Cause and effect diagrams can be used for any problem.

A cause and effect diagram starts by creating the line and the ultimate effect. In Figure 4-2, the effect is the outage. Then you add additional items (the causes), making the diagram look similar to a fishbone. You can expand the diagram for any of the elements. For example, you could expand "attack" to include specific types of attacks. Attacks may include malware, DoS, buffer overflow, or other types of attacks.

NOTE
The cause and effect diagram is also called an *Ishikawa diagram*, or a *fishbone diagram*. It is used to link problems with causes.

When creating a cause and effect diagram, you can run out of ideas or focus on a single topic. To balance the diagram, consider the following five elements. You're not required to include all the elements. However, you can use any of them to help identify causes:

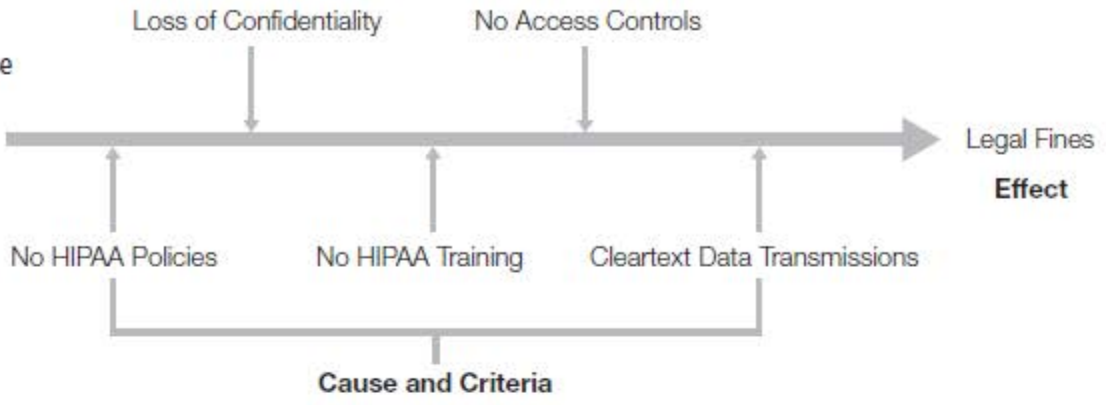
- **Methods**—What methods could contribute to an outage?
- **Machinery**—What machinery issues could contribute to an outage?
- **Manpower**—What manpower issues could contribute to an outage?
- **Materials**—What material issues could contribute to an outage?
- **Environment**—What environmental issues could contribute to an outage?

Figure 4-3 shows another example of a cause and effect diagram. In this example, the cause is loss of confidentiality. The remaining items show the criteria that can allow the loss of data. For HIPAA, the effect can be substantial fines.

Recommendation Cost and Time Frame

In addition to the findings, the report will include a list of recommendations. These recommendations will address the potential causes and criteria that can result in the negative effect.

FIGURE 4-3
HIPAA compliance cause and effect diagram.



Each item should include the cost required to implement it. Also include the timeline to implement the solution. Management will use this data to decide if the solution should be applied.

For example, the following partial list of recommendations could be included in the Web site risk management plan:

- **Upgrade firewall**—Initial cost: $4,000. Ongoing costs: $1,000 annually.
  The initial cost will cover the purchase of the firewall. The ongoing costs are related to training and maintenance.
  Purchase and install the firewall within 30 days of approval.
- **Purchase and install IDS**—Initial cost: $1,500. Ongoing costs: negligible.
  Purchase and install the IDS within 30 days of approval.
- **Create plan to keep system updated**—Initial cost: manpower.
  Ongoing costs: manpower.
  Purchase and install the system within 30 days of approval.
- **Install antivirus software on server**—Initial cost: $75. Ongoing costs: negligible.
  Purchase and install the software within 30 days of approval.

Cost Estimate Accuracy

Because a CBA is only as valuable as its cost estimates, it's important to get accurate data. However, this can be difficult. It helps to understand how data can be skewed.

Costs for solutions are often underestimated. For example, ongoing costs may not be included in the initial cost estimates. A product that looks easy to manage may require expensive training.

The success of a solution can be overestimated. A solution may be expected to reduce incidents by 90 percent. In practice, the reduction may be closer to 50 percent.

There are times when personnel don't have a vested interest in providing accurate information. For example, sales personnel interested in an initial sale may sometimes gloss over ongoing costs. You can also expect them to stress the most positive aspects of their products.

- **Update antivirus software**—Initial cost: negligible. Ongoing costs: negligible.
  Configure antivirus software for automatic updates after installation.
- **Add one IT administrator**—Cost: negotiated salary. Due to the ongoing maintenance requirements of these recommendations, an additional administrator is required.

> **NOTE**
> The individual ongoing costs may be small, but the cumulative requirements may be more. In this example, the time required to maintain these solutions may justify an additional administrator.

Cost-Benefit Analysis

The CBA is a process used to determine how to manage a risk. If the benefits of a control outweigh the costs, the control can be implemented to reduce the risk. If the costs are greater than the benefits, the risk can be accepted.

In this context, the CBA should include two items:

- **Cost of the recommendation**—The recommendation is the control intended to manage the risk. If you anticipate that there will be ongoing costs, you should include them in the calculation.
- **Projected benefits**—Calculate benefits in terms of dollars. Benefits can be expressed as money earned or losses reduced.

Management is responsible for making the decisions on how to manage the risks. An accurate CBA allows management to make intelligent decisions.

Here is a sample CBA for a Web site recommendation:

- **Recommendation**—Install antivirus (AV) software on the Web server.
- **Cost of the recommendation**—$75.
- **Background**—AV software was not installed on the Web server in the past because of performance concerns. Malware infected the Web server several times in the past year. These infections caused multiple outages on the Web server. The total downtime was five hours. The Web server generates approximately $500 per 15 minutes of uptime, or $2,000 per hour. AV software is expected to prevent 90 percent of infections.
- **Loss before AV software**—$30,000. Outages resulted in $10,000 of direct loss of revenue ($2,000 × 5 hours). Indirect losses are estimated to be $20,000. This includes the advertising costs to bring back lost customers.
- **Expected loss with AV software**—$3,000. The AV software is expected to reduce the losses by 90 percent ($30,000 − ($30,000 × .9) = $3,000).
- **Benefit of AV software**—$27,000 ($30,000 × .9 = $27,000).
- **CBA**—$26,925. The CBA is calculated as:
  - Loss Before AV Software − Loss After AV Software − Cost of AV Software
  - $30,000 − $3,000 − $75 = $26,925

You can't overestimate the importance of accurate data. The key to completing an accurate CBA is starting with accurate data. Again, this is sometimes difficult to get. It often requires digging below the surface to determine costs.

Probing questions can often uncover flaws in the data. Consider the following scenarios and questions:

- If a control is said to reduce losses by 90 percent, you can ask, "How did you arrive at 90 percent?"
- If the cost of a control is given, you can ask, "Does this include any ongoing costs?"

Probing questions don't need to be accusatory. The goal isn't to create a conflict. Instead, the goal is to validate the data. Questions should be asked with a tone of "help me understand." If the data is flawed, the presenter can easily get defensive. On the other hand, if the data is valid, the presenter can answer questions with facts to support the claims.

Risk Statements

Reports are often summarized in **risk statements**. You use risk statements to communicate a risk and the resulting impact. They are often written using "if/then" statements. The "if" part of the statement identifies the elements of the risk. The "then" portion of the statement identifies the effect.

For example, the following risk statement could be used for the Web site:

- If AV software is not installed on the Web server, then the likelihood that the server will become infected is high. The Web server has a constant connection to the Internet.
- If the server is infected, then an outage is likely to occur. Any outage will result in $500 of lost sales for every 15 minutes of downtime.

You should be able to match the risk statements to the scope and objectives of the project. If the statement isn't within the scope or objectives, the risk assessment may be off track. You'll then need to go back and focus the findings or the recommendation.

Documenting Management Response to Recommendations

After you present your managers with the recommendations, they will decide what to do. They can accept, defer, or modify recommendations:

- **Accept**—Management approves the recommendation. Approved recommendations are funded and implemented. They will then be added to a POAM for tracking.
- **Defer**—Management can also defer a recommendation. It may still be implemented at a later time. However, do not include it in the list of accepted recommendations.

- **Modify**—Management can also decide to modify a recommendation. For example, you may recommend a firewall. Management may decide on two firewalls to implement a demilitarized zone (DMZ). On the other hand, you may recommend a $4,000 firewall. Management may decide to purchase an $800 firewall instead.

> **NOTE**
> A demilitarized zone (DMZ) is commonly used to protect Internet-facing servers. It usually consists of two firewalls. One firewall filters traffic from the Internet to the DMZ. The other firewall filters traffic from the internal network to the DMZ.

Documenting and Tracking Implementation of Accepted Recommendations

It's important to document the decisions made by management. As time passes, the decisions can become distorted if you don't document them. This is especially true if the recommendations are deferred or modified.

Imagine you managed the risk management plan for the Web site. The plan recommended purchase of AV software, but this recommendation was deferred. Three months later, the system is infected with malware. A four-hour outage results in losses exceeding $8,000. You may be asked why the software wasn't purchased.

If you documented the decisions, this is a simple matter to address. Without documentation, the result may be uncomfortable finger-pointing.

The documentation doesn't need to be extensive. It could be a simple document listing the recommendation and the decision. It could look similar to this:

- **Recommendation to purchase AV software**—Accepted
  Software is to be purchased as soon as possible.
- **Recommendation to hire an IT administrator**—Deferred
  IT department needs to provide clearer justification for this. In the interim, the IT department is authorized to use overtime to ensure security requirements are met.
- **Recommendation to purchase SS75 firewall**—Modified
  Two SS75 firewalls are to be purchased as soon as possible. These two firewalls will be configured as a DMZ.

Plan of Action and Milestones

> **NOTE**
> A POAM is sometimes abbreviated as POA&M.

A **plan of action and milestones (POAM)** is a document used to track progress. POAMs are used in many types of project management. A POAM is used to assign responsibility and to allow management follow-up:

- **Assignment of responsibility**—The POAM makes it clear who is responsible for each task. When a task is not completed on schedule, it also makes clear whom to hold accountable.
- **Management follow-up**—PMs and upper-level management can use the POAM to follow up on a project. The POAM allows managers to quickly determine the status of any project. When project management tools are used, the source of the problem is often easy to identify.

POAMs are also useful for any audited projects. For example, HIPAA requires regular reviews. The POAM can show the progress the company has made to become compliant. If a company is not 100 percent compliant but can show it has made significant progress, fines may be waived or reduced. If a company doesn't have any documentation indicating progress, maximum fines could be assessed.

There are no specific formats required for a POAM. One company may create a POAM in a Microsoft Excel spreadsheet with 15 columns for every item. Another company may create a POAM in a Microsoft Word document.

The POAM is a living document. It is not a report that is created once and is complete. Instead, you should update the POAM throughout the life cycle of a project. Additionally, the POAM may look different depending on the phase of the project. Early in the project, the POAM may be generic. Later in the project, it could be more specific.

For example, consider the Web site risk management plan. The Web site has been attacked. It has suffered two major outages in the last two months. The cause of these two incidents is probably well known. However, all the threats and vulnerabilities are probably not known. The initial POAM might have the following generic items:

- **Approve risk management plan:** Assigned to _____ Due by _____
- **Identify threats:** Assigned to _____ Due by _____
- **Identify vulnerabilities:** Assigned to _____ Due by _____
- **Identify potential solutions:** Assigned to _____ Due by _____
- **Prepare risk management plan report:** Assigned to _____ Due by _____
- **Approve risk response plan:** Assigned to _____ Due by _____
- **Begin implementation of plan:** Assigned to _____ Due by _____
- **Complete implementation of plan:** Assigned to _____ Due by _____

Later, when management approves the specific recommendations, you can create a POAM for the approved and modified recommendations. Each recommendation within the POAM could have multiple line items. For example, the task of upgrading the firewall could be a major milestone. When all of the tasks are completed, the milestone is met.

- **Log current firewall activity:** Assigned to _____ Due by _____
- **Purchase two SS75 firewalls:** Assigned to _____ Due by _____
- **Create firewall policy:** Assigned to _____ Due by _____
- **Test firewalls:** Assigned to _____ Due by _____
- **Implement external firewall:** Assigned to _____ Due by _____
- **Implement internal firewall:** Assigned to _____ Due by _____
- **Move Web server to DMZ:** Assigned to _____ Due by _____

NOTE

A **milestone** is a scheduled event. It indicates the completion of a major task or group of tasks. Milestones are commonly used in project management to verify how the project is doing. When milestone dates are missed, the project is behind schedule.

Project Management Software

There are many different versions of project management software available. One example is Microsoft Office Project. It includes different versions such as Microsoft Office Project Standard and Project Professional.

Project software includes additional tools that can be used to create charts. Charting tools provide a graphical representation of the project. They can also automatically detect the status of a project.

Some software will indicate the status of a project with colors such as green, yellow, or red. Green could indicate on schedule and on budget. Yellow could indicate a danger of going overschedule or overbudget. Red could indicate overschedule or overbudget.

A PM can enter data as the risk management project progresses. These charts will automatically be updated. It's also possible to use a server to host data on multiple projects. Managers can access reports on any of the projects via a Web browser.

Each line item could include the following details:

- Task name
- Associated threat or vulnerability
- Risk level (low, medium, or high)
- Step or milestone name
- Assignment of responsibility
- Point of contact
- Estimated cost
- Actual cost
- Estimated person hours to complete task
- Actual person hours to complete task
- Scheduled start date
- Actual start date
- Milestone due date
- Current status
- Scheduled completion date
- Actual date of completion
- Comments

You can use different tools to assist in tracking the POAM. These tools don't replace the POAM but instead provide graphical representations of the POAM and its progress. These tools include:

- Milestone plan chart
- Gantt chart
- Critical path chart

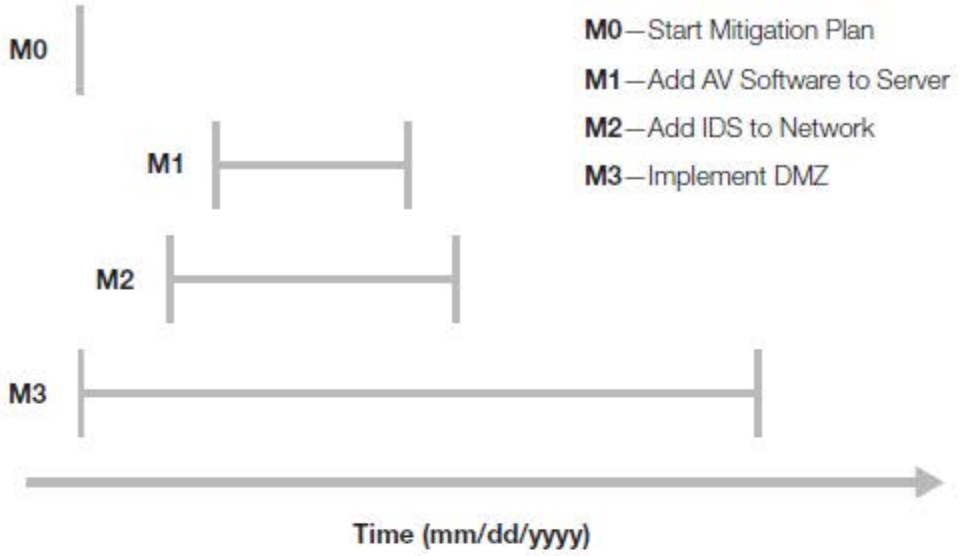


FIGURE 4-4
Milestone plan chart.

Charting the Progress of a Risk Management Plan

Managers often use charts to show the progress of a risk management plan. Charts provide a graphical representation of key information. As the saying goes, "a picture is worth a thousand words." Similarly, a chart is worth a thousand words. The following sections cover some of the common charts managers use to track a plan's progress.

Milestone Plan Chart

A **milestone plan chart** is a simple graphical representation of major milestones. It shows the major milestones laid out in a graphical format. If there are any dependencies between the milestones, this chart will show them. In other words, if milestone 2 can't begin until milestone 1 has been completed, this chart will show this dependency.

It's also common to include actual start and end dates in the chart. Figure 4-4 shows an example of a milestone plan chart.

The milestone plan chart can also help allocate resources. For example, the tasks in Figure 4-4 aren't dependent on one another. However, you can see that the tasks are staggered. It's possible for each task to start at the same time. However, if the same person or same department will perform all of the tasks, it may not be possible to start each one at the same time.

In this case, start the longest task milestone first. In the figure, the M3 milestone will implement a DMZ and is the longest. Once you order the firewalls, you can start another task while waiting for the firewall to arrive. M2 can start at that point. Once you order the IDS software, you can start milestone M1.

This chart can also help management change the priority of any of the milestones. The installation of AV software may be considered the most important first step. The figure shows that the M1 is being delayed so that M3 can start first. This can be changed so M1 starts first with an accepted delay in the implementation of the DMZ.

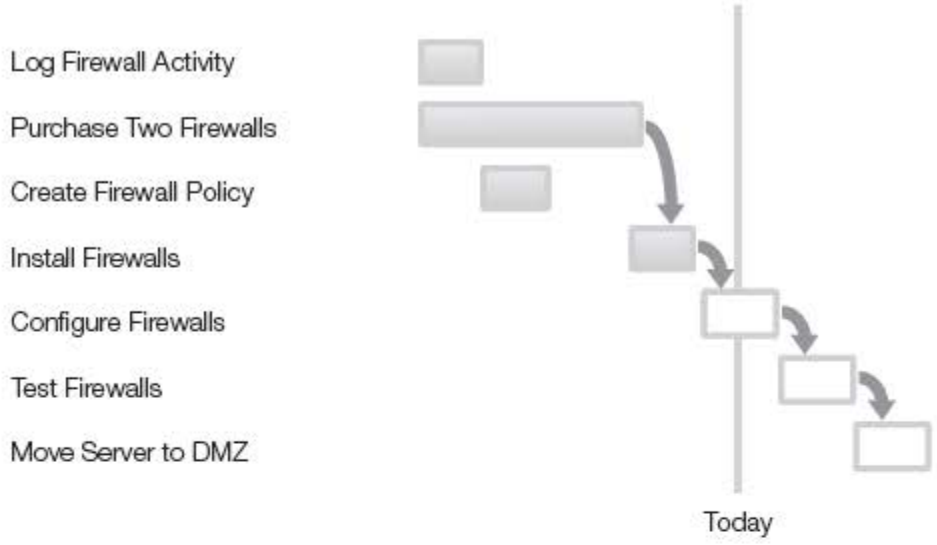


FIGURE 4-5
Gantt chart.

Gantt Chart

A **Gantt chart** shows a project schedule. Gantt charts are commonly used in project management. The primary difference between the milestone plan chart and the Gantt chart is that the Gantt chart shows more detail.

Figure 4-5 shows an example of a Gantt chart. The shaded items show the tasks that have been completed. Notice that the Gantt chart is showing the detailed steps for the implementation of the DMZ.

The Gantt chart allows any manager to quickly view the progression and status of the project. In the figure, all of the tasks that were supposed to be completed before today are complete. The PM needs only to focus on the task in progress or future tasks.

> **NOTE**
> The Gantt chart was developed by Henry Gantt. He worked with the Army Bureau of Ordnance during World War I. He realized that processes could be controlled easier if they were broken down into smaller elements. As the often repeated saying goes: "How do you eat an elephant? One bite at a time."

On the other hand, if previous tasks weren't completed, the PM can quickly identify where to focus attention. For example, if the firewalls weren't installed yet, the Install Firewalls task would not be shaded. The PM could see this element is past due and address the issue.

Most project management software automates the creation of Gantt charts. Additionally, as the tasks in the project are completed, it will automatically indicate completion in the chart. Before computers were so popular, these charts would be filled in by hand.

Critical Path Chart

Some tasks within a project can be delayed without impacting the project finish date. Other tasks must be completed on time. A **critical path chart** shows a list of project tasks that must be completed on time. If any task in the path is delayed, the overall project will be delayed.

FIGURE 4-6
Critical path chart.

For example, you cannot install a firewall until the firewall is purchased. If the purchase is delayed, the installation will be delayed. These two items would be in the critical path. On the other hand, you can delay creating a log of current firewall activity. As long as the delay isn't too long, it won't impact the overall schedule.

Figure 4-6 shows an example of a critical path chart. This is the critical path for the firewall project.

Compare Figures 4-5 and 4-6. Notice that two tasks are missing in Figure 4-6. Log Firewall Activity and Create Firewall Policy are not in the critical path. If these two tasks are slightly delayed, they will not delay the entire project. The only requirement is that they be completed before the Install Firewalls task starts.

CHAPTER SUMMARY

A risk management plan is a specific type of project plan. The project is to identify and mitigate risks. You start by creating objectives and a project scope. You then identify risks. Finally, you create a response plan as recommendations to mitigate the risks. Management can then choose to accept, defer, or modify the risks.

You then implement the recommendations. A primary tool used to track the recommendations is a plan of action and milestones (POAM). This POAM is a living document that is updated throughout the project. You can supplement it with different charting tools to ease project management tasks.

KEY CONCEPTS AND TERMS

Affinity diagram
Brainstorming
Cause and effect diagram
Critical path chart
Firewall
Firewall appliance
Firewall policy
Gantt chart
Milestone
Milestone plan chart
Plan of action and milestones (POAM)
Risk statements
Scope
Scope creep
Stakeholder

CHAPTER 4 ASSESSMENT

1. What are valid contents of a risk management plan?

A. Objectives
B. Scope
C. Recommendations
D. POAM
E. All of the above

2. What should be included in the objectives of a risk management plan?

A. A list of threats
B. A list of vulnerabilities
C. Costs associated with risks
D. Cost-benefit analysis
E. All of the above

3. What will the scope of a risk management plan define?

A. Objectives
B. POAM
C. Recommendations
D. Boundaries

4. What problem can occur if the scope of a risk management plan is not defined?

A. Excess boundaries
B. Stakeholder loss
C. Scope creep
D. SSCP

5. What is a stakeholder?
   A. A mark that identifies critical steps
   B. An individual or group that has an interest in the project
   C. A critical process or procedure
   D. Another name for the risk management plan project manager

6. A key stakeholder should have authority to make decisions about a project. This includes authority to provide additional resources.
   A. True
   B. False

7. A risk management plan project manager oversees the entire plan. What is the project manager responsible for? (Select two.)
   A. Ensuring costs are controlled
   B. Ensuring the project stays on schedule
   C. Ensuring stakeholders have adequate funds
   D. Ensuring recommendations are adopted

8. A risk management plan includes steps to mitigate risks. Who is responsible for choosing what steps to implement?
   A. The project manager
   B. Management
   C. Risk management team
   D. The POAM manager

9. A risk management plan includes a list of findings in a report. The findings identify threats and vulnerabilities. What type of diagram can document some of the findings?
   A. Gantt chart
   B. Critical path chart
   C. POAM diagram
   D. Cause and effect diagram

10. What three elements should be included in the findings of the risk management report?
    A. Causes, criteria, and effects
    B. Threats, causes, and effects
    C. Criteria, vulnerabilities, and effects
    D. Causes, criteria, and milestones

11. What is a primary tool used to identify the financial significance of a mitigation tool?
    A. Ishikawa diagram
    B. Fishbone diagram
    C. CBA
    D. POAM

12. A fishbone diagram can link causes with effects.
    A. True
    B. False

13. You present management with recommendations from a risk management plan. What can management choose to do?
    A. Accept or reject the recommendations
    B. Adjust, defer, or modify the recommendations
    C. Accept, defer, or modify the recommendations
    D. Allow or deny the recommendations

14. What is a POAM?
    A. Project objectives and milestones
    B. Planned objectives and milestones
    C. Project of action milestones
    D. Plan of action and milestones

15. A POAM is used to track the progress of a project. What type of chart is commonly used to assist with tracking?
    A. Fishbone chart
    B. Cause and effect chart
    C. Gantt chart
    D. POAM chart