CHAPTER 4

The Drivers of the Information Security Business

EVERY ORGANIZATION CARRIES OUT TASKS to satisfy business objectives. Without objectives, organizations have no purpose. You must identify the elements in your organization that support your business objectives. These elements are your organization's **business drivers**. Business drivers include people, information, and conditions that support business objectives. Information security activities directly support several common business drivers, including compliance and efforts to protect intellectual property. Security activities can also negatively affect business drivers, making it more difficult to satisfy your business objectives.

Some outside requirements direct how your organization carries out its tasks. These requirements can come from legislation, regulation, industry demands, or even your own standards. Every organization has some requirements with which it must comply. There are multiple ways that your organization can meet requirements. Most regulations require that you develop plans to handle business interruptions or disasters. In fact, most activities that restore operations after an interruption support several requirements.

Always consider different controls to satisfy compliance requirements. It's important that you balance security activities with their impact on your business drivers to protect your information's security. In this chapter, you will learn about security-related business drivers and how they support your overall business drivers.

Chapter 4 Topics

This chapter covers the following topics and concepts:

- What risk management is
- How BIA, BCP, and DRP differ from one another, and how they are the same
- How to assess the impact of risks, threats, and vulnerabilities
- How to close the information security gap
- How to mitigate risk and achieve compliance with laws, regulations, and requirements
- How to maintain A-I-C compliance

Chapter 4 Goals

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

- Define risk management and the way organizations should approach risk management
- Distinguish BIA, BCP, and DRP from one another and compare them to one another
- Assess the impact of risks, threats, and vulnerabilities on the IT infrastructure
- Define an acceptable level of risk or liability
- Shrink the information security gap based on risk-mitigation strategies
- Adhere to compliance laws and governance (policies, standards, procedures, and guidelines)
- Manage and mitigate risk as part of ongoing security operations
- Determine how to comply with A-I-C goals that are defined for your IT infrastructure

Defining Risk Management

Risk management is the process of identifying, assessing, prioritizing, and addressing risks. Any organization that is serious about security will view risk management as an ongoing process.

Risk management is not something you do just once. Each part of the risk-management process is separate but can occur many times. Risk management ensures that you have planned for risks that are most likely to have an effect on your organization. A secure organization has plans in place to address risks *before* events occur.

In Chapter 1, you learned that risk is the probability that an uncertain event will affect one or more resources. Most people view risks only in terms of negative effects. However, the **Project Management Body of Knowledge (PMBOK)**, maintained by the **Project Management Institute (PMI)**, states that the effects of risk can be positive or negative. PMI bases its risk-management philosophy on a proactive approach, which simultaneously does the following:

- Minimizes the effects of negative risks
- Maximizes the effects of positive risks

Consider the classic view of risks. Figure 4-1 shows the classic relationship between risks, threats, and vulnerabilities.

As shown in Figure 4-1, the risk equation is as follows:

Risk = Threats × Vulnerabilities.

A threat is the frequency of any event. In most cases, the events in the threat equation are negative or adverse events. Vulnerability is the likelihood that a specific threat will successfully be carried out. Multiplying the probability of a threat and the likelihood of a vulnerability yields the risk of that particular event. Risks apply to specific assets. If you multiply the risk probability by the cost of the asset, the result is the exposure to a specific risk.

Many people have never thought of risk as being a positive thing. However, uncertainty can result in events that have negative *or* positive effects. For example, suppose your organization plans to deploy new software to your end users based on projected availability from your software vendor. Your risk-management plan should address the responses to both an early and a late software delivery. If you receive the software early, you can either perform more exhaustive testing or begin deployment early. If your software vendor is late delivering software to you, you may miss your projected deployment date. You should have plans in place to address both the positive and negative effects of a delivery date that does not match your schedule.

A **risk methodology** is a description of how you will manage risk. The risk methodology that your organization adopts should include the approach, required information, and the techniques to address each risk. The approach defines how you will carry out the steps of the risk-methodology process. For example, the approach could state that risk analysis will be conducted at specified intervals. The tools for conducting this analysis can include

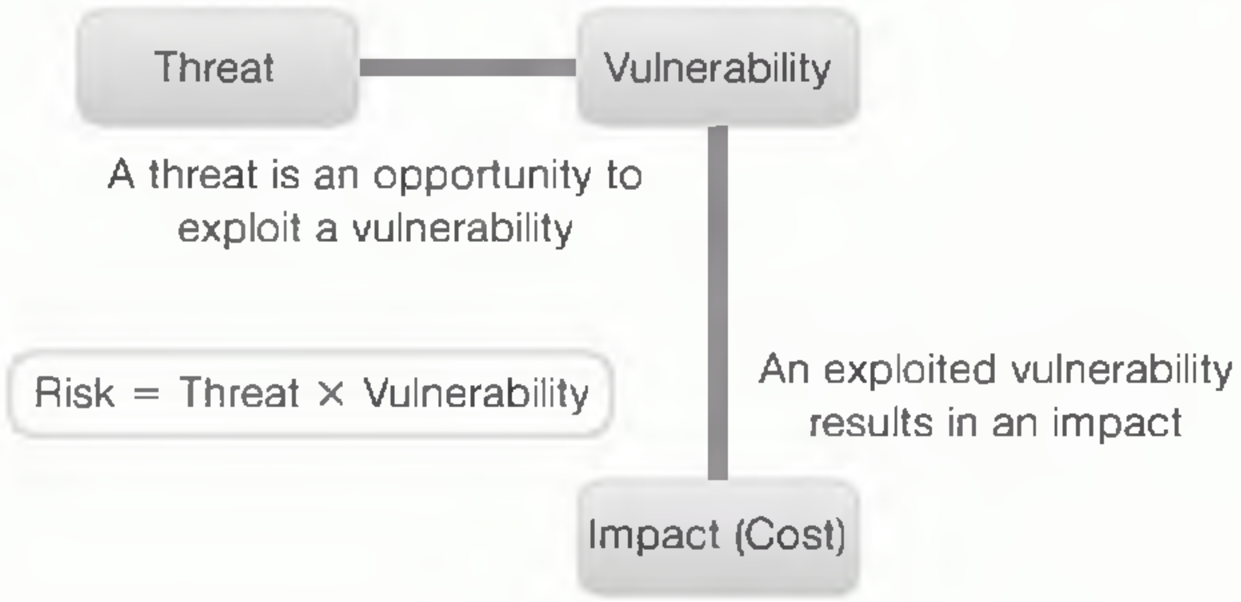

Threat
Vulnerability
A threat is an opportunity to exploit a vulnerability
Risk = Threat × Vulnerability
An exploited vulnerability results in an impact
Impact (Cost)

FIGURE 4-1 Risks, threats, and vulnerabilities.

the documents that define, categorize, and rank risks. This approach is consistent with PMI's PMBOK. While the PMI approach isn't the only way to do things, it does provide a prescriptive approach to project management in general, including risk management.

The process of managing risks starts by identifying risks. According to PMI, the steps in the risk-management process are as follows:

- Risk identification
- Risk analysis
- Risk-response planning
- Risk monitoring and control

Risk Identification

Risk identification is the process of determining and classifying the risks that might affect your resources. The ability to identify risks is a key part of an effective risk-management process. Identifying risks should involve as many people working in different roles as possible. Having more people involved enables you to identify risks from multiple perspectives.

The result of the risk identification process is a list of identified risks. PMI calls this list the **risk register**. The risk register can contain many different types of information, but should contain at least the following:

- A description of the risk
- The expected impact if the associated event occurs
- The probability of the event occurring
- Steps to mitigate the risk
- Steps to take should the event occur
- Rank of the risk

You might fill in only part of the risk register during this phase. This goal is to document as many risks as possible. Having too many risks in the risk register is much better than overlooking any severe risk that does occur. You can collect input for the risk register in several ways, including the following:

- Risk-identification brainstorming meetings
- Formal surveys
- Informal polls and requests for comments
- Incentivized events, such as "lunch and learn" sessions that include a forum for collecting comments and feedback

NOTE

Offering gifts or free food generally encourages a free flow of feedback.

Your organization's ability to respond to any risk starts with how well you identify potential risks. Be creative when asking for risk-register input. Using multiple perspectives will give you a more complete response plan.

It's crucial to ensure you have the support of your organization's upper management. Without management's support, you'll likely lack the authority to carry out the steps needed to develop a good risk-management plan. You will enjoy the benefits of having full management support from the very beginning in these risk-identification activities. Don't bring in management as an afterthought.

As the process of collecting information continues, more and more people should become involved. Larger groups can discourage participants from speaking up about weaknesses within your organization, however. They may fear reprisal, or fear that others will view them as complainers. You may find that one technique in particular produces the candid results you need: the **Delphi method**. This is an approach to using formal anonymous surveys in multiple rounds to collect opinions and information. Because the surveys are anonymous, the method encourages candid responses. A panel reviews each round of survey responses and creates a new survey based on the results of the previous round. Multiple rounds allow you to focus on areas of concern and assemble detailed information from a number of subject-matter experts.

Risk Analysis

The next step is to analyze the identified risks to decide how to rank them. All organizations have limited budgets. They cannot respond to every potential risk. Risk analysis allows organizations to decide which risks require more attention than others do. You shouldn't waste time and resources to mitigate risks that aren't likely to occur and will cause only minimal damage if they do. Mitigating risks that are likely to occur and may cause substantial damage makes the most sense.

Organizations use two common approaches to analyze risk:

- Qualitative risk analysis
- Quantitative risk analysis

Qualitative Risk Analysis

Qualitative risk analysis uses relative ranking to determine risk responses. This technique uses risk probability and risk impact. Risk probability is important because it measures how likely it is a risk will occur. When conducting a qualitative risk assessment, you generally express risk probability as a relative likelihood. You typically express risk probabilities as follows:

- **High probability**—Very likely to occur
- **Average probability**—Neither frequent nor rare
- **Low probability**—Not very likely to occur

A high-probability risk deserves more attention than a low-probability risk.

Another way to assess risk is by risk impact. Risk impact is a measure of how a risk will affect the organization or project. Risk impact can range from low (negligible) to high (substantial). A risk with low impact requires a different response than one with a high impact.

Different organizations may choose different classifications for risk probability and risk impact. Qualitative risk analysis quickly prioritizes risks to conduct response planning and further risk analysis.

Quantitative Risk Analysis

Quantitative risk analysis is another risk-analysis method. It uses mathematical formulas and numbers to rank risk severity. The goal of quantitative risk analysis is to quantify possible outcomes of risks, determine probabilities of outcomes, identify high-impact risks, and develop plans based on risks. Although quantitative risk analysis can be a complex topic, the basic idea is to consider several qualities of risks and the resources the risk may affect.

You can use quantitative risk analysis for all risks on the risk register, but the amount of effort required may be overkill for low-probability or low-impact risks. For this reason, quantitative risk analysis generally starts with those risks you consider high probability during qualitative risk analysis.

Here are the steps involved in performing a quantitative risk analysis for each item on your risk register:

1. Calculate the risk exposure.
   a. Assign a value to each resource.
   b. Determine the percentage of loss for each realized threat. This value is the **exposure factor (EF)** for the threat against a resource.
2. Calculate the loss for a single threat occurrence, called the **single loss expectancy (SLE)**, using the following formula:

   SLE = resource value × EF
3. Calculate or determine the annual probability of a loss. The estimated annual probability that a stated threat will be realized is called the **annual rate of occurrence (ARO)**.
4. Calculate the annual estimated loss due to a specific realized threat, called the **annual loss expectancy (ALE)**, using the following formula:

   ALE = SLE × ARO

TABLE 4-1 Quantitative risk analysis.

RESOURCE	RISK	VALUE	EF	SLE	ARO	ALE
Building	Fire	$700,000	0.60	$420,000	0.20	$ 84,000
File server	Disk crash	$ 50,000	0.50	$ 25,000	0.20	$ 5,000
Sensitive data	Theft	$200,000	0.90	$180,000	0.70	$126,000
E-business Internet connection	Unavailability for one hour	$ 15,000	1.00	$ 15,000	12.00	$180,000

Table 4-1 contains a few sample risks and the calculated ALE for each risk. Once you have an ALE for each risk, you can determine which risks to address first.

Risk-Response Planning

After you identify and rank as many risks as possible, the next step is to select strategies to address each risk. You should include these strategies in the risk register. Your risk-response plan shows that you have examined risks to your organization and have developed plans to address each risk. It's important that you include a response description for every risk on the risk register. Ignoring a risk is not a valid option. You should assign one or more "owners" to each risk response to carry out the planned actions.

> **NOTE**
>
> Responding to a risk of any type does not make the risk go away. The risk still exists. Any risk that exists but has a defined response is called a **residual risk**.

There are four responses to negative risks:

- **Avoid**—When you avoid a negative risk, you eliminate the threat by changing resources or the IT infrastructure. For example, you might avoid the risk of a single point of failure for your Internet connection by adding additional gateway devices.
- **Transfer**—When you transfer a negative risk, you shift it to a third party. For example, purchasing fire insurance shifts the associated risk to the company holding the policy.
- **Mitigate**—When you mitigate a negative risk, you reduce the probability or the impact of the risk. For example, to mitigate known attacks, you can harden Web servers by updating software and changing configuration settings.
- **Accept**—When you accept a negative risk, you take no steps in response to that risk. You might accept a risk if the effects of the risk are not worth the expense of a response. An example of a risk you might accept is an unencrypted network connection between your database server and application server. Because setting up an encrypted connection between the two servers involves a cost in terms of both dollars and performance, and because it's very unlikely that an attacker will threaten this network connection, your organization can simply accept the risk.

For positive risks, the responses include the following:

- **Exploit**—When you exploit a positive risk, you take advantage of an opportunity that arises when you respond to that risk. For example, suppose your organization developed training materials for use within your organization to help you address a specific risk. You might exploit the risk by packaging and marketing those training materials to other organizations.
- **Share**—When you share a positive risk, you use a third party to help capture the opportunity associated with that risk. For example, purchasing a group of workstation licenses along with another organization enables both organizations to realize a substantial discount due to the size of the combined order. (In this case, the risk is that the license cost may change.)

- **Enhance**—When you enhance a positive risk, you increase the probability or positive impact of the event associated with the risk. For example, suppose you have a contract to deliver software that includes a $20,000 bonus for early completion. To enhance the positive risk—a delivery date that does not match your schedule—you might offer a subcontractor you've hired a $5,000 bonus for finishing ahead of the deadline.
- **Accept**—When you accept a positive risk, you take no steps to address it because the potential effects of the risk are positive and add value. For example, suppose you have purchased a new automated backup and configuration utility that can help your organization deploy new workstations in half the allotted time. Because the utility is new, it may take some time to learn—meaning it may *not* help your organization save any time deploying new workstations. It's determined that at worst, learning the new utility and using it to manage deployments will take the same amount of time as doing it manually. However, if you realize the positive risk, you will finish the deployments sooner than planned.

Risk Monitoring and Control

You shouldn't perform risk identification and analysis just once. Conditions within an organization constantly change, as do the risks encountered by the organization. You must continually monitor risks and perform additional analysis to develop new risk responses any time you identify new risks. The formal process of monitoring and controlling risk focuses on identifying and analyzing new risks. It also focuses on tracking previously identified risks.

You should reevaluate risks when any of the following events occur:

- You identify evidence that a threat has been realized or is about to be realized.
- Your organization approves a change request to your risk-response plan.
- Any changes occur to your environment that may affect resource risks.
- You apply corrective or preventive actions.

You should continually ensure that your risk-management plan matches your current environment. If your environment changes in any way, you should reevaluate risks to ensure you are best prepared to handle any threats.

Implementing a BIA, a BCP, and a DRP

The primary focus of risk management is to preempt realized threats. It's not possible to foresee and prevent every event that results in loss. That means that the likelihood still exists that any organization will encounter an event that will interrupt normal business operations. Information security requires all information to be available when any authorized user needs it. You'll have to develop and implement methods and techniques for protecting the organization's IT resources and ensuring that events do not interrupt normal business functions.

Business Impact Analysis

The first step in developing plans to address interruptions is to identify those business functions that are crucial to your organization. Some of your organization's activities are critical to the operation of the business and some aren't. When an event interrupts your organization's ability to conduct operations, it's important to restore the most crucial operations first. Before you can do this, you have to identify what those functions are.

A business impact analysis (BIA) is a formal analysis of an organization's functions and activities that classifies them as critical or noncritical. Critical functions are required to run the business. If you cannot carry out a critical function, it causes unacceptable damage. Noncritical functions may be important, and you might miss them if they did not exist, but their absence would not stop an organization from conducting business. A BIA also arranges critical activities based on importance and helps an organization determine which functions to restore in what order if there is a major interruption.

In the BIA, the section for each critical function receives additional information, including a description of recovery goals and requirements for each function. Recovery goals and requirements are expressed as follows:

- **Recovery point objective (RPO)**—The amount of data loss that is acceptable. Depending on the nature of the function, staff members may be able to re-create or reenter data. The RPO provides direction on whether loss prevention or loss correction is a better option.
- **Recovery time objective (RTO)**—The maximum allowable time to recover the function. Many less formal recovery plans overlook RTO. Time may be a critical factor, and specifying the requirements for recovery time helps determine the best recovery options.
- **Business recovery requirements**—Any business prerequisites for the functions—that is, other business functions that must already be in place for the recovery functions to occur. Business recovery requirements help in determining the recovery sequence.
- **Technical recovery requirements**—Any technical prerequisites to support each business function. In most cases, technical recovery requirements dictate which IT infrastructure components must be in place.

Ensuring that operations and functions that are critical to an organization are able to continue is crucial to the organization's survival. The BIA will help identify not only which functions are critical, but also how quickly essential business functions must return to full operation following a major interruption. It will also identify resource requirements for returning each function to full operation. BIAs generally assume a worst-case scenario in which the physical infrastructure supporting each activity or function has been destroyed, along with any data. You can choose to plan for any interruption timeframe, but in many BIAs, restoration plans assume that access to primary resources will not be possible for at least 30 days. In other words, a solid BIA will indicate the requirements necessary to conduct business for an extended period when the normal infrastructure is unavailable.

Business Continuity Plan

A business continuity plan (BCP) is a plan for a structured response to any events that result in an interruption to critical business activities or functions. Performing a BIA is an important first step toward generating a BCP in that the BIA identifies the resources for which a BCP is necessary.

There is generally no reason to develop a BCP for resources that aren't crucial to an organization's survival. The BCP primarily addresses the processes, resources, equipment, and devices needed to continue conducting critical business activities when an interruption occurs that affects the business's viability.

The most important part of any BCP is setting priorities, with the understanding that people always come first. There are no exceptions. Any plan that addresses business interruptions and disasters must place the safety and well-being of the organization's people as the highest priority. All other concerns are secondary. The order of priorities for a well-balanced BCP should be as follows:

- Safety and well-being of all people
- Buildings and facilities
- Infrastructure components, including communications and information systems

You must address the needs of each category before continuing to the next category. If conditions are hazardous for humans, they can't do anything productive. If your people are safe but your building is damaged, you can't replace servers or network hardware. You must wait for the damage to be repaired or for the organization to be relocated to restore infrastructure components. Keep the order of resource priority in mind as you develop plans to avoid business-process interruptions.

A formal BCP isn't just helpful for many organizations—in some circumstances, it's required. Legislation and regulations often require a BCP to ensure systems are safe. Today's organizations increasingly rely on IT resources and require a solid IT infrastructure to conduct business. The cost for system downtime for these companies can be extreme. Direct and indirect costs associated with downtime can exist in several categories, including:

NOTE

Direct costs are immediate expenditures that reduce profit. Indirect costs, such as losing a customer, affect the overall revenue stream but are harder to calculate because there is no expenditure record. In the case of indirect costs, the impact is that potential sales just never happen.

- Lost customers
- Lost revenue
- Lost market share
- Additional expenses
- Damaged reputation

Organizations must consider contingency and recovery plans from a comprehensive perspective. Plans cannot focus on individual resources to the exclusion of others. While each of the components of contingency and recovery plans do generally address specific resources, they must do so within a larger context. Keeping the larger context in view during plan development enables you to address the risks to an organization as opposed to just fixing a broken resource.

Elements of a complete BCP should include the following:

- Emergency response and protection of life and safety
- Situation and damage assessment
- Resource salvage and recovery
- Alternate facilities for emergency operation and business recovery

Briefly, a BCP directs all activities required to ensure that an organization's critical business functions continue with little or no interruption. The BCP assumes that the infrastructure components needed to support operations are in place. Unfortunately, that is not always the case after a disaster. What happens when a fire destroys your data center? How can you continue business operations in that case? The answer is, you need another plan: a disaster recovery plan (DRP).

Disaster Recovery Plan

A disaster recovery plan (DRP) directs the actions necessary to recover resources after a disaster. A DRP is part of a BCP. It is necessary to ensure the restoration of resources required by the BCP to an available state. The DRP extends and supports the BCP by identifying events that could cause damage to resources that are necessary to support critical business functions. The BCP already contains a list of the resources necessary to support each business function. The next step in developing a DRP is to consider what could happen to each resource.

Threat Analysis

A threat analysis involves identifying and documenting threats to critical resources. Before you can recover from a disaster, you need to consider what types of disasters are possible and what types of damage they can cause. For example, recovering from a data-center fire is different from recovering from a flu epidemic. Some common threats include the following:

- Fire
- Flood
- Hurricane

BCP Versus DRP: What's the Difference?

What is the difference between a BCP and a DRP? A BCP does not specify how to recover from disasters, just interruptions. In general, an *interruption* is a minor event that may disrupt one or more business processes for a short period. In contrast, a *disaster* is an event that affects multiple business processes for an extended period. Disasters often also cause substantial resource damage that you must address before you can resolve the business process interruption.

- Tornado
- Disease
- Earthquake
- Cyberattack
- Sabotage
- Utility outage
- Terrorism

With the exception of disease, each of these threats has the potential to damage an organization's infrastructure. In contrast, disease directly affects personnel. You can address disease with various solutions. If, however, the disease affects people charged with carrying out the recovery plans, the recovery may be unsuccessful.

Note that these threats do not necessarily occur one at a time. One threat may lead to another threat. For example, a flood that introduces contaminated water into an office may lead to disease that incapacitates your staff. As another example, a tornado or earthquake could also result in a fire. Always assume that disasters may occur in groups, not only as single events.

Impact Scenarios

After defining potential threats, the next step in creating a comprehensive DRP is to document likely impact scenarios. These form the basis of the DRP. In most organizations, planning for the most wide-reaching disaster rather than focusing on smaller issues results in a more comprehensive plan. Narrowing the focus on smaller issues can result in a DRP that fails to consider a broader strategy. A broader strategy is necessary to recover from the loss of multiple resources simultaneously. An impact scenario like "Building Loss" will likely encompass all critical business functions and the worst potential outcome from any given threat. A DRP may include additional impact scenarios if an organization has more than one building.

A solid DRP might also contain additional, more-specific impact scenarios. For example, your plan may include a scenario that addresses the loss of a specific floor in a building. Many plans underestimate the resources necessary to move from one location to another. Don't neglect the resources necessary to execute each step of your plan. A recovery plan that fails just because you didn't have access to a truck large enough to move your equipment to an alternate site isn't a very solid plan.

Recovery Requirement Documentation

Once you complete the analysis phase, you should document the business and technical requirements to initiate the implementation phase. You'll likely need access to asset information, including asset lists and their availability during a disaster. Each asset has an owner. The owner of an asset must grant access to it to the disaster relief team. Including at least one member of upper management in BIA, BCP, and DRP planning can help you head off political battles for control over assets during disasters.

The asset information you'll likely need to develop a DRP includes the following:

- The number, types, and locations of desks and other office furniture that can be used to furnish a secondary location
- Personnel necessary for the recovery effort, along with their contact information and their roles in the recovery process
- Application software and data required for critical business functions
- Resources necessary for manual workaround solutions
- Maximum allowable outage time and data loss for each software application
- Required peripherals, such as printers, copiers, fax machines, and other office equipment

Disaster Recovery

It's important to train all personnel on the proper response to any disaster. A common mistake is to be too eager to begin the recovery process. Even though your organization has devoted substantial time and resources to developing a DRP, you must ensure that you react to the disaster, not the plan. The critical steps in responding to a disaster include the following:

- **Ensure everyone's safety first**—No resource is as important as people are.
- **Respond to the disaster before pursuing recovery**—Required response and containment actions depend on the nature of the disaster and may not have anything to do with the recovery effort.
- **Follow the DRP, including communicating with all affected parties**—Once your people are safe and you have responded to the disaster, you can pursue recovery actions.

Disaster recovery is an extension to the DRP. It addresses recovering from common system outages or interruptions. A disaster is generally larger than a common outage, and the resources may not be available to enact simple recovery solutions. For example, most database-management systems enable you to quickly recover the primary database from a replicated copy. However, if a disaster has resulted in the destruction of your database server computer, you'll have to restore the server to a stable state before you can restore your database data.

A disaster may render your data center unusable, forcing you to relocate your operations. Careful planning for such a move makes it viable. Although moving your data center to another location may not sound like a major undertaking, it involves many details—which is why you should devote so much effort to planning. You must install hardware and software, and there are network and telecommunications requirements. Table 4-2 lists several common data-center options for disaster recovery.

TABLE 4-2 Data center alternatives for disaster recovery.

OPTION	DESCRIPTION	COMMENTS
Hot site	Facility with environmental utilities, hardware, software, and data that closely mirrors the original data center	Most expensive option, least switchover time
Warm site	Facility with environmental utilities and basic computer hardware	Less expensive than a hot site, but requires more time to load operating systems, software, data, and configurations
Cold site	Facility with basic environmental utilities but no infrastructure components	Least expensive option, but at the cost of the longest switchover time since all hardware, software, and data must be loaded at the new site
Mobile site	Trailer with necessary environmental utilities that can operate as a warm site or cold site	Very flexible, fairly short switchover time, and widely varying costs based on size and capacity

It may be to your advantage to work out a mutual aid agreement with another company where each organization agrees to provide backup resources in the event of a disaster. The agreement could include after-hours access to computing resources or physical space to use as a temporary data center. Carefully examine all the requirements when considering a cooperative agreement. Providing basic critical functionality for a data center may seem straightforward, but some resources, such as telecommunication service, may not be easy to switch from one location to another. Also, consider how close any alternate location is to your existing location. If your proposed alternate location is too close to your main location, a large disaster such as a flood or an earthquake could affect both.

NOTE

In some industries, cooperative agreements are mandatory. For example, banks are required to maintain cooperative agreements with other banks. They are also required to regularly test their ability to use other banks' facilities to ensure uninterrupted service to their customers.

Disaster recovery is rapidly becoming an increasingly important aspect of enterprise computing. As business environments become more complex, more things can go wrong. Recovery plans have become more complex to keep up. DRPs vary from one organization to another, depending on many factors. These include the type of organization, the processes involved, and the level of security needed. Most enterprises remain unprepared or underprepared for a disaster. And despite recurrent reminders, many companies do not have a DRP at all. Of those that do, nearly half have never tested their plan—which is essentially the same as not having one.

It's crucial to validate your DRP for effectiveness and completeness, and test it for accuracy. It's rare that the first version of a DRP is complete and correct. You must test your DRP to identify weaknesses. You can engage a disaster-recovery firm to assist in such tests. These tests can range from simple reviews to complete disaster simulations. The most effective tests simulate real disasters, including transferring software between computer systems and ensuring that you can establish communications at an alternate location. Following are various different types of DRP tests:

- **Checklist test**—This is the simplest type of DRP test. In a checklist test, each participant follows steps on the DRP checklist and provides feedback. You can use checklist tests for DRP training and awareness.
- **Structured walkthrough**—A structured walkthrough is similar to a checklist test, but the DRP team uses role-playing to simulate a disaster and evaluate the DRP's effectiveness. This type of test is also called a tabletop exercise or conference-room test.
- **Simulation test**—A simulation test is more realistic than a structured walkthrough. In a simulation test, the DRP team uses role-playing and follows through with as much of the effects of a simulated disaster as possible without affecting live operations.
- **Parallel test**—A parallel test evaluates the effectiveness of the DRP by enabling full processing capability at an alternate data center without interrupting the primary data center.
- **Full-interruption test**—This is the only complete test. Full-interruption tests interrupt the primary data center and transfer processing capability to an alternate site.

Not all aspects of DRPs are reactive. Some parts of a DRP are preventative and intended to avoid the negative effects of a disaster in the first place. Preventative components of a DRP may include some of the following:

- Local mirroring of disks systems and use of data-protection technology such as a redundant array of independent disks (RAID)
- Surge protectors to minimize the effect of power surges on delicate electronic equipment
- Uninterruptible power supply (UPS) and/or a backup generator to keep systems going in the event of a power failure
- Fire-prevention systems
- Antivirus software and other security controls

Assessing Risks, Threats, and Vulnerabilities

One of the first steps in developing a comprehensive BCP and DRP is to fully assess the risks, threats, and vulnerabilities associated with your organization's critical resources. You can't protect your environment from every possible threat, so it's necessary to prioritize. Until you know the risks, you can't know which remedies are necessary.

TABLE 4-3 Common risk-assessment methodologies.

NAME	DESCRIPTION	FOR MORE INFORMATION
Risk Management Guide for Information Technology Systems (NIST SP 800-30 and SP 800-66)	Part of the Special Publication 800 series reports, these products provide detailed guidance of what you should consider in risk management and risk assessment in computer security. The reports include checklists, graphics, formulas, and references to U.S. regulatory issues. NIST SP 800-66 specifically addresses HIPAA concerns.	*http://www.csrc.nist.gov*
CCTA Risk Analysis and Management Method (CRAMM)	CRAMM is a risk analysis method developed by the British government. Best practices of British government organizations are the basis of the first releases of the CRAMM method and tool. People around the world use CRAMM. CRAMM is also the British government's preferred risk analysis method. CRAMM is best suited for large organizations.	*http://www.cramm.com*
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)	The OCTAVE approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach. There are two versions of OCTAVE: OCTAVE and OCTAVE-S. OCTAVE is best suited for large organizations, whereas OCTAVE-S works well for organizations consisting of fewer than 100 people.	*http://www.cert.org/octave/osig.html*
ISO/IEC 27005 "Information Security Risk Management"	An ISO standard that describes information security risk management in a generic manner. The documents include examples of approaches to information security risk assessment and lists of possible threats, vulnerabilities, and security controls.	*http://www.iso.org/*

There are many approaches to assessing risk. Each organization conducts the process in its own unique way. Instead of starting from scratch in the risk-assessment process, you can use one of the many methodologies that are available. At least one of these is likely a good fit for your organization. Investing the time to research the various offerings can make the whole process more effective and efficient. Table 4-3 lists common risk-assessment methodologies.

Closing the Information Security Gap

In spite of all best efforts, no collection of security controls is perfect. There are always some vulnerabilities for which there are no controls. The difference between the security controls you have in place and the controls you need in order to address all vulnerabilities is called the **security gap**.

A valuable tool to help ensure you are satisfying your organization's security policy is a **gap analysis**. From an IT security perspective, a gap analysis is a comparison of the security controls you have in place and the controls you need in order to address all identified threats. Gap-analysis activities should be ongoing. They should consist of regular reviews of day-to-day practices vis-à-vis the latest threat assessment. Threats that you do not address through at least one control indicate gaps in your security.

Gap analysis is an effective method for gauging the overall security of an organization's IT environments. In addition, gap analysis can provide assurances that security implementations are consistent with real requirements. You can conduct many different types of gap-analysis activities. They can be formal investigations or informal surveys. Factors that influence the analysis include the size of your organization, the industry in which you operate, the cost involved, efforts involved, and the depth of the analysis.

Many of the following steps are common when conducting a gap analysis:

- Identifying the applicable elements of the security policy and other standards
- Assembling policy, standard, procedure, and guideline documents
- Reviewing and assessing the implementation of the policies, standards, procedures, and guidelines
- Collecting inventory information for all hardware and software components
- Interviewing users to assess knowledge of and compliance with policies
- Comparing the current security environment with policies in place
- Prioritizing identified gaps for resolution
- Documenting and implementing the remedies to conform to policies

One important aspect of gap analysis is determining the cause of the gap. The fact that a gap exists means there is a lack of adequate security controls, but *why* does the gap exist? There are several common reasons for security gaps in any organization, such as:

- Lack of security training, resulting in noncompliant behavior
- Intentional or negligent disregard of security policy
- Unintended consequence of a control or policy change

- Addition or modification of hardware or software without proper risk analysis
- Configuration changes that lack proper risk analysis
- Changes to external requirements, such as legislation, regulation, or industry standards that require control changes

As you can see, most security gaps relate closely to user actions. One of the first steps you can take to close gaps is to ensure that you fully train personnel on security issues. Well-trained people are your best allies in securing your IT environment. As your security efforts become more sophisticated and your organization's personnel become more security savvy, you should encounter fewer and fewer security gaps.

Adhering to Compliance Laws

The last 20 years have seen an explosion in computing power and in the number of ways computers are used. The increased reliance on networked resources, hardware, and software has created many new opportunities for the malicious use of resources. Information has become a valued asset to organizations and an attractive target to attackers. As information-related crime has grown, so has legislation and regulation to protect organizations and individuals from criminal activity.

Today's organizations are increasingly subject to various laws enacted to protect the privacy of electronic information. Each organization must comply with laws and regulations, although the specific laws and regulations to which an organization is subject depend on its location, the type of information it handles, and the industries in which it operates.

The following list summarizes many of the most far-reaching laws and regulations that affect how organizations conduct IT operations:

- **Sarbanes-Oxley Act (SOX)**—Sarbanes-Oxley, which became law in July of 2002, introduced sweeping changes to how corporate governance and financial practices are regulated. As a direct result of several public financial scandals, SOX established the Public Company Accounting Oversight Board (PCAOB), which is responsible for overseeing, regulating, inspecting, and disciplining accounting firms in their roles as auditors of public companies. SOX also dictates policies that address auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure.
- **Health Insurance Portability and Accountability Act (HIPAA)**—HIPAA, which took effect on April 14, 2006, governs how doctors, hospitals, and other health care providers handle personal medical information. HIPAA requires that all medical records, billing, and patient information be handled in ways that maintain the patient's privacy. HIPAA also guarantees that all patients be able to access their own medical records, correct errors or omissions, and be informed of how personal information is used. To ensure every affected person is aware of HIPAA's requirements, patients must receive notifications of privacy procedures any time they submit medical information.

- **Federal Information Security Management Act (FISMA)**—FISMA officially recognizes the importance of information security to the national security and economic health of the United States. FISMA requires every federal agency to develop and maintain formal information security programs, including security awareness efforts; secure access to computer resources; strict acceptable use policies; and formal incident response and contingency planning.
- **Gramm-Leach-Bliley Act (GLBA)**—GLBA addresses information security concerns in the financial industry. GLBA requires that financial institutions provide their clients a privacy notice that explains what information the company gathers about the client, where the information is shared, and how the company protects that information. Companies must provide clients with this privacy notice prior to entering into an agreement to do business.
- **Payment Card Industry Data Security Standard (PCI DSS)**—Although not a law, PCI DSS affects any organization that processes or stores credit card information. The founding payment brands of the PCI Security Standards Council—including American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International—developed PCI DSS to foster consistent global data-security measures. The PCI DSS is a comprehensive security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.
- **The Family Education Rights and Privacy Act (FERPA)**—This federal law protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Under FERPA, schools must receive written permission from a parent or eligible student before releasing any information contained in a student's education record.
- **USA Patriot Act of 2001**—Passed 45 days after the September 11, 2001, attacks on the World Trade Center in New York City and on the Pentagon in Washington, D.C., the Patriot Act substantially expanded the authority of U.S. law-enforcement agencies to enable them to fight terrorism in the United States and abroad. It expands the ability of law-enforcement agencies to access information that pertains to an ongoing investigation.
- **Children's Online Privacy Protection Act of 1998 (COPPA)**—COPPA restricts how online information is collected from children under 13 years of age. It dictates what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children's privacy and safety online.
- **Government Information Security Reform Act (Security Reform Act) of 2000**—This act focuses on management and evaluation of the security of unclassified and national security systems. It formalized existing Office of Management and Budget (OMB) security policies and restated security responsibilities contained in the Computer Security Act of 1987.

- **California Database Security Breach Act of 2003**—This California act, along with several other similar state acts, requires any company that stores customer data electronically to notify its customers any time there is a security breach. The company must immediately notify any affected customers if someone breaches its computer system and steals unencrypted information. Other similar bills limit the ability of financial institutions to share nonpublic personal client information with affiliates and third parties.

It's the responsibility of each organization to understand which laws and regulations apply to them and to employ necessary controls to comply. This effort often requires frequent attention and results in audits and assessments to ensure the organization remains compliant.

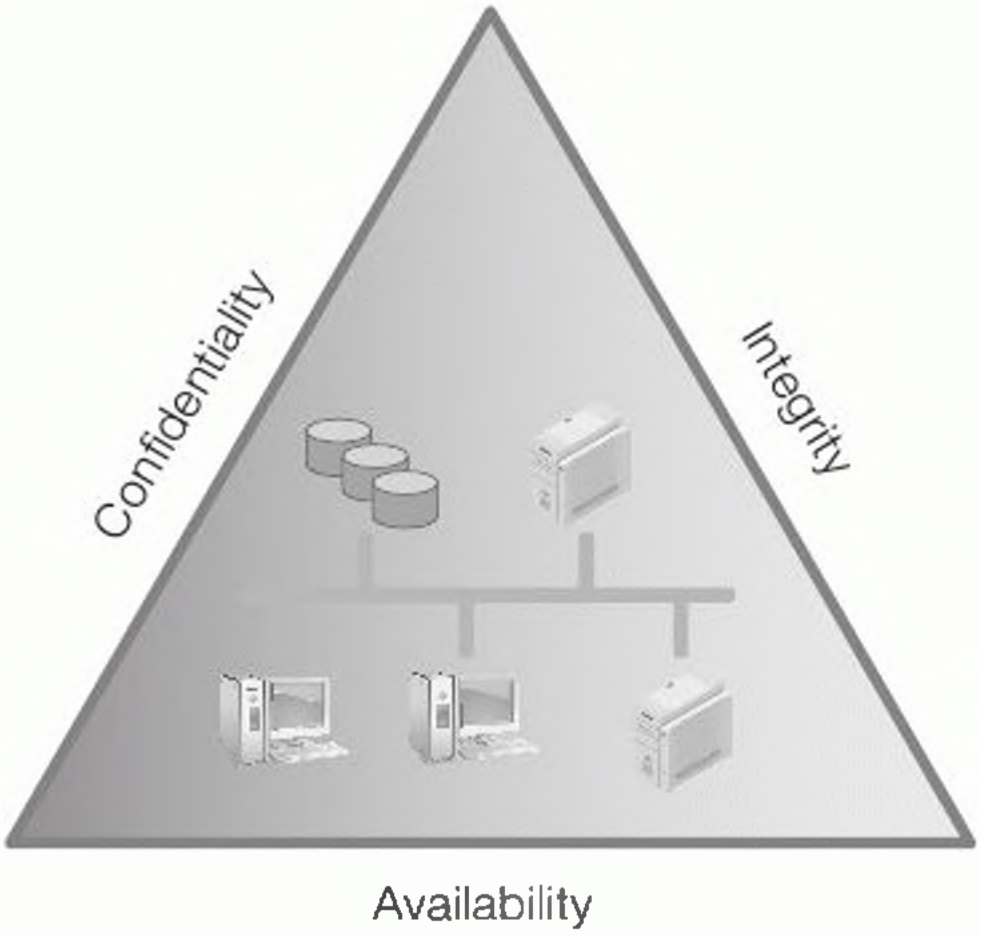
Keeping Private Data Confidential

Many of the compliance requirements you saw in earlier sections address data confidentiality. One of the most important classes of security controls is those that keep information confidential. Ensuring availability and integrity is important, but confidentiality gets the most attention. That's because you cannot undo a confidentiality violation. That is, once someone views confidential data, there is no way to remove it from his or her memory. You must pay careful attention to each of the three tenets of information security to protect your organization's data assets. Figure 4-2 shows the three tenets of information security.

You will learn different techniques in this book to ensure the availability, integrity, and confidentiality of data. At the highest level, data is secure when it is available to authorized users and not available to unauthorized users. You will have to cover many details before you can fully ensure your data's security. Maintaining confidentiality will certainly be a recurring theme. In fact, many controls to ensure confidentiality also ensure other aspects of data security.

FIGURE 4-2

The three tenets of information security.



As you learn more about various security controls, you will see how they work together to protect data from unauthorized use. Most strategies to secure data use a three-pronged approach that includes the techniques of authentication, authorization, and accounting. These three techniques help ensure that only authorized users can access resources and data. They also ensure that enough information is captured to troubleshoot access issues after the access occurs. Investigations into security incidents rely on accounting information to reconstruct past events.

The basic purpose of the three-pronged approach is to maintain security by preventing unauthorized use of any protected resource. Many authentication and access controls can help accomplish this task. Some of the authentication controls you will learn about include the following:

- Passwords and PINs
- Smart cards and tokens
- Biometric devices
- Digital certificates
- Challenge-response handshakes
- Kerberos authentication
- One-time passwords

NOTE

In the context of monitoring information system activity, the term **accounting** means recording events in log files. You can use computer-event accounting to trace users' actions and determine a sequence of events that is helpful when investigating incidents.

Once you have authenticated a user, access controls help ensure only authorized users can access the protected resource. Authorization controls you will learn about include the following:

- Authentication server rules and permissions
- Access control lists
- Intrusion detection and prevention
- Physical access control
- Connection and access policy filters
- Network traffic filters

These two lists give a brief overview of some of the security controls that help to ensure your organization's data security. You will learn about the details and implementation techniques of these controls in upcoming chapters.

CHAPTER SUMMARY

In this chapter, you learned that security is much more than a way to keep data secret. Security is an integral part of any organization. A solid security policy ensures that an organization can perform its primary business functions even in the event of a disaster and will do so while protecting all of its assets, including its data. The same solid security policy provides the assurance that the organization has employed the necessary controls to comply with all necessary laws, regulations, and other security requirements. In short, security keeps an organization viable and allows it to conduct business.

KEY CONCEPTS AND TERMS

Accounting
Annual loss expectancy (ALE)
Annual rate of occurrence (ARO)
Business drivers
Delphi method
Exposure factor (EF)
Gap analysis
Project Management Body of Knowledge (PMBOK)
Project Management Institute (PMI)
Qualitative risk analysis
Quantitative risk analysis
Residual risk
Risk management
Risk methodology
Risk register
Security gap
Single loss expectancy (SLE)

CHAPTER 4 ASSESSMENT

1. Risk management is responding to a negative event when it occurs.

   A. True
   B. False

2. With respect to IT security, a risk can result in either a positive or a negative effect.

   A. True
   B. False

3. According to PMI, which term describes the list of identified risks?

   A. Risk checklist
   B. Risk register
   C. Risk methodology
   D. Mitigation list

4. Which type of risk analysis uses formulas and numerical values to indicate risk severity?

   A. Objective risk analysis
   B. Qualitative risk analysis
   C. Subjective risk analysis
   D. Quantitative risk analysis

5. Which type of risk analysis uses relative ranking?

   A. Objective risk analysis
   B. Qualitative risk analysis
   C. Subjective risk analysis
   D. Quantitative risk analysis

6. Which risk-analysis value represents the annual probability of a loss?

   A. EF
   B. SLE
   C. ALE
   D. ARO

7. Which risk-response option would best describe purchasing fire insurance?

   A. Accept
   B. Mitigate
   C. Transfer
   D. Avoid

8. Which risk response would be most appropriate if the impact of a risk becoming a reality is negligible?

   A. Accept
   B. Mitigate
   C. Transfer
   D. Avoid

9. Which of the following statements best describes the relationship of a BCP to a DRP?

   A. A BCP is required but a DRP is not
   B. A DRP is a component of a BCP
   C. A DRP is required but a BCP is not
   D. A BCP is a component of a DRP

10. Which term is used to indicate the amount of data loss that is acceptable?

    A. RAI
    B. ROI
    C. RTO
    D. RPO

11. A(n) ________ identifies processes that are critical to the operation of a business.

12. Which risk-assessment methodology is marketed as a self-directed approach and has two different editions for organizations of different sizes?

    A. CRAMM
    B. OCTAVE
    C. NIST
    D. EBIOS

13. ________ is the U.S. security-related act that governs health-related information.

14. Which U.S. security-related act governs the security of data specifically for the financial industry?

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