chapter 20

Risk Management

A ship is safe in harbor, but that's not what ships are for.

—William Shedd

In this chapter, you will learn how to

- **Use risk management tools and principles to manage risk effectively**
- **Explain the differences between qualitative and quantitative risk assessment**
- **Describe essential risk management tools**

Risk management can best be described as a decision-making process. In the simplest terms, when you manage risk, you determine what could happen to your business, you assess the impact if it were to happen, and you decide what you could do to control that impact as much as you or your management deems necessary. You then decide to act or not to act, and, finally, you evaluate the results of your decision. The process may be iterative, as industry best practices clearly indicate that an important aspect of effectively managing risk is to consider it an ongoing process.

Cross Check

Change Management and Risk Management Are Critical Management Tools

Risk management is one of the reasons behind change management. Change management is a process designed to enable management efforts to understand implications of changes prior to incorporation in production systems. When someone requests a change to production, do they have answers to questions such as these:

1. What are the security implications of this change?
2. What is the back-out plan in the event the change causes unintentional problems?

For more detail, the reader is directed to Chapter 21, which explains details of change management as a critical management tool.

An Overview of Risk Management

Risk management is an essential element of management from the enterprise level down to the individual project. Risk management encompasses all the actions taken to reduce complexity, increase objectivity, and identify important decision factors. There has been, and will continue to be, discussion about the complexity of risk management and whether or not it is worth the effort. Businesses must take risks to retain their competitive edge, however, and as a result, risk management must occur as part of managing any business, program, or project.

Risk management is both a skill and a task that is performed by all managers, either deliberately or intuitively. It can be simple or complex, depending on the size of the project or business and the amount of risk inherent in an activity. Every manager, at all levels, must learn to manage risk. The required skills can be learned.

Risk management is about making a business profitable— not about buying insurance.

Exam Tip: This chapter contains several bulleted lists. These are designed for easy memorization in preparation for taking the Security+ exam.

Example of Risk Management at the International Banking Level

The Basel Committee on Banking Supervision comprises government central-bank governors from around the world. This body created a basic, global risk management framework for market and credit risk. It implemented internationally a flat 8 percent capital charge to banks to manage bank risks. In layman's terms, this means that for every $100 a bank makes in loans, it must possess $8 in reserve to be used in the event of financial difficulties. However, if banks can show they have very strong risk mitigation procedures and controls in place, that capital charge can be reduced to as low as $0.37 (0.37 percent). If a bank has poor procedures and controls, that capital charge can be as high as $45 (45 percent) for every $100 the bank makes. See www.bis.org/bcbs/ for source documentation regarding the Basel Committee.

This example shows that risk management can be and is used at very high levels—the remainder of this chapter focuses on smaller implementations and demonstrates that risk management is used in many aspects of business conduct.

Risk Management Vocabulary

You need to understand a number of key terms to manage risk successfully. Some of these terms are defined here because they are used throughout the chapter. This list is somewhat ordered according to the organization of this chapter. More comprehensive definitions and other pertinent terms are listed alphabetically in the glossary at the end of this book.

Risk **Risk** is the possibility of suffering harm or loss.

Risk management **Risk management** is the overall decision-making process of identifying threats and vulnerabilities and their potential impacts, determining the costs to mitigate such events, and deciding what actions are cost effective for controlling these risks.

Risk assessment **Risk assessment** is the process of analyzing an environment to identify the risks (threats and vulnerabilities) and mitigating actions to determine (either quantitatively or qualitatively) the impact of an event that would affect a project, program, or business. Also referred to as **risk analysis**.

Tech Tip

Types of Controls

Controls can be classified based on the types of actions they perform. Three classes of controls exist:

- *Management orAdministrative*
- *Technical*
- *Operational orPhysical*

For each of these classes, there are four types of controls:

- *Preventive (deterrent)*
- *Detective*
- *Corrective (recovery)*
- *Compensating*

Asset An **asset** is any resource or information an organization needs to conduct its business.

Threat A **threat** is any circumstance or event with the potential to cause harm to an asset. For example, a malicious hacker might choose to hack your system by using readily available hacking tools.

Vulnerability A **vulnerability** is any characteristic of an asset that can be exploited by a threat to cause harm. Your system has a security vulnerability, for example, if you have not installed patches to fix a cross-site scripting (XSS) error on your web site.

Impact **Impact** is the loss resulting when a threat exploits a vulnerability. A malicious hacker (the threat) uses an XSS tool to hack your unpatched web site (the vulnerability), stealing credit card information that is used fraudulently. The credit card company pursues legal recourse against your company to recover the losses from the credit card fraud (the impact).

Control A **control** is a measure taken to detect, prevent, or mitigate the risk associated with a threat. Also called **countermeasure** or **safeguard**.

Qualitative risk assessment **Qualitative risk assessment** is the process of subjectively determining the impact of an event that affects a project, program, or business. Completing the assessment usually involves the use of expert judgment, experience, or group consensus.

Quantitative risk assessment **Quantitative risk assessment** is the process of objectively determining the impact of an event that affects a project, program, or business. Completing the assessment usually involves the use of metrics and models.

Mitigate The term **mitigate** refers to taking action to reduce the likelihood of a threat occurring.

Single loss expectancy (SLE) The **single loss expectancy (SLE)** is the monetary loss or impact of each occurrence of a threat exploiting a vulnerability.

Exposure factor **Exposure factor** is a measure of the magnitude of loss of an asset. Used in the calculation of single loss expectancy.

Annualized rate of occurrence (ARO) **Annualized rate of occurrence (ARO)** is the frequency with which an event is expected to occur on an annualized basis.

Annualized loss expectancy (ALE) **Annualized loss expectancy (ALE)** is how much an event is expected to cost per year.

The distinction between qualitative and quantitative risk assessment will be more apparent as you read the section "Qualitative vs. Quantitative Risk Assessment" later in the chapter.

Exam Tip: These terms are important, and you should completely memorize their meanings before taking the Security+ exam.

What Is Risk Management?

Three definitions relating to risk management reveal why it is sometimes considered difficult to understand:

- The dictionary defines *risk* as the possibility of suffering harm or loss.
- Carnegie Mellon University's Software Engineering Institute (SEI) defines *continuous risk management* as "processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to 1) assess continuously what could go wrong (risks); 2) determine which risks are important to deal with; and 3) implement strategies to deal with those risks" (SEI, *Continuous Risk Management Guidebook* [Pittsburgh, PA: Carnegie Mellon University, 1996], 22).
- The Information Systems Audit and Control Association (ISACA) says, "In modern business terms, risk management is the process of identifying vulnerabilities and threats to an organization's resources and assets and deciding what countermeasures, if any, to take to reduce the level of risk to an acceptable level based on the value of the asset to the organization" (ISACA, *Certified Information Systems Auditor (CISA) Review Manual, 2002* [Rolling Meadows, IL: ISACA, 2002], 344).

These three definitions show that risk management is based on what can go wrong and what action should be taken, if any. Figure 20.1 provides a macro-level view of how to manage risk.

Tech Tip

Risk Management Applies to All Business Processes

Even Human Resource Management relies on risk management. For example, risk management used to say that older workers could create liabilities. Recent studies have shown that as the workforce ages, it has become apparent that older workers have lower absenteeism, are more productive, and have higher levels of job satisfaction. Their greatest risk is longer recovery time from accidents—companies are finding ways to prevent accidents to manage that risk.

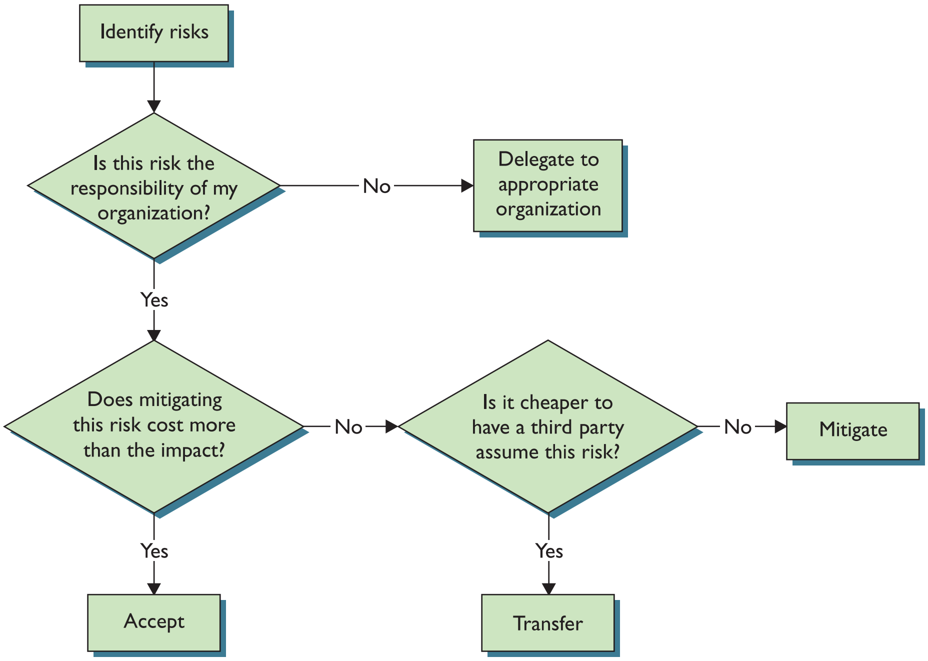

Identify risks
Is this risk the responsibility of my organization?
No
Delegate to appropriate organization
Yes
Does mitigating this risk cost more than the impact?
No
Is it cheaper to have a third party assume this risk?
No
Mitigate
Yes
Accept
Yes
Transfer

Figure 20.1 A planning decision flowchart for risk management

Business Risks

No comprehensive identification of all risks in a business environment is possible. In today's technology-dependent business environment, risk is often simplistically divided into two areas: business risk and, a major subset, technology risk.

Tech Tip

Transferring Risk

One possible action to manage risk is to transfer that risk. The most common method of transferring risk is to purchase insurance. Insurance allows risk to be transferred to a third party that manages specific types of risk for multiple parties, thus reducing the individual cost.

Examples of Business Risks

Following are some of the most common business risks:

- **Treasury management** Management of company holdings in bonds, futures, currencies, and so on.
- **Revenue management** Management of consumer behavior and the generation of revenue.
- **Contract management** Management of contracts with customers, vendors, partners, and so on.
- **Fraud** Deliberate deception made for personal gain, to obtain property or services, and so on.
- **Environmental risk management** Management of risks associated with factors that affect the environment.
- **Regulatory risk management** Management of risks arising from new or existing regulations.

- **Business continuity management** Management of risks associated with recovering and restoring business functions after a disaster or major disruption occurs.
- **Technology** Management of risks associated with technology in its many forms.

Examples of Technology Risks

Following are some of the most common technology risks:

- **Security and privacy** The risks associated with protecting personal, private, or confidential information.
- **Information technology operations** The risks associated with the day-to-day operation of information technology systems.
- **Business systems control and effectiveness** The risks associated with manual and automated controls that safeguard company assets and resources.
- **Business continuity management** The risks associated with the technology and processes to be used in event of a disaster or major disruption.
- **Information systems testing** The risks associated with testing processes and procedures of information systems.
- **Reliability and performance management** The risks associated with meeting reliability and performance agreements and measures.
- **Information technology asset management** The risks associated with safeguarding information technology physical assets.
- **Project risk management** The risks associated with managing information technology projects.
- **Change management** The risks associated with managing configurations and changes (see Chapter 21).

It is important that you understand that technology, itself, is a business risk. Hence, it must be managed along with other risks. Today, technology risks are so important they should be considered separately.

Tech Tip

Risk According to the Basel Committee

The Basel Committee referenced earlier in the chapter has defined three types of risk specifically to address international banking:

- ***Market risk*** *Risk of losses due to fluctuation of market prices*
- ***Credit risk*** *Risk of default of outstanding loans*
- ***Operational risk*** *Risk from disruption by people, systems, processes, or disasters*

Risk Management Models

Risk management concepts are fundamentally the same despite their definitions, and they require similar skills, tools, and methodologies. Several models can be used for managing risk through its various phases. Two models are presented here: the first can be applied to managing risks in general, and the second is tailored for managing risk in software projects.

General Risk Management Model

The following five steps can be used in virtually any risk management process. Following these steps will lead to an orderly process of analyzing and mitigating risks.

Tech Tip

Key Performance Indicators (KPIs)

The development of KPIs to monitor performance of systems and processes is critical to effective risk management. If you can't measure it, you have to rely on more subjective measures. Examples of KPIs for an enterprise resource planning (ERP) system such as Oracle E-Business Suite or SAP Business Suite could include:

Business KPI	***Measures Growth of the Number of…***
GL Business Unit growth	*General Ledger (GL) Business Units (BUs) over time*
AP Business Unit growth	*Accounts Payable (AP) BUs over time*
Purchasing Business Unit growth	*Purchasing BUs over time*
Project Costing Business Unit growth	*Project Costing BUs over time*
Asset Mgt Business Unit growth	*Asset Mgt BUs over time*
GL Transaction growth	*GL Transactions in major tables over time*
GL Journal Header growth	*GL Journal Header entries over time*
GL Journal Line growth	*Journal Line entries over time*
AP Voucher Header growth	*AP Voucher Header entries over time*
AP Voucher Line growth	*AP Voucher Line entries over time*
PO Transaction growth	*Purchase Order (PO) Transactions over time*
PO Line Transaction growth	*PO Line Transactions over time*
Asset Mgt Transaction growth	*Asset Mgt Transactions over time*

Step 1. Asset Identification

Identify and classify the assets, systems, and processes that need protection because they are vulnerable to threats. Use a classification that fits your business. This classification leads to the ability to prioritize assets, systems, and processes and to evaluate the costs of addressing the associated risks. Assets can include

- Inventory
- Buildings
- Cash
- Information and data
- Hardware
- Software
- Services
- Documents
- Personnel
- Brand recognition
- Organization reputation
- Goodwill

Step 2: Threat Assessment

After identifying the assets, you identify both the possible threats and the possible vulnerabilities associated with each asset and the likelihood of their occurrence. Threats can be defined as any circumstance or event with the potential to cause harm to an asset. Common classes of threats include (with examples):

- **Natural disasters** Hurricane, earthquake, lightning, and so on.
- **Man-made disasters** Earthen dam failure, such as the 1976 Teton Dam failure in Idaho; car accident that destroys a municipal power distribution transformer; the 1973 explosion of a railcar containing propane gas in Kingman, Arizona.
- **Terrorism** The 2001 destruction of the World Trade Center, the 1995 gas attack on the Shinjuku train station in Tokyo.
- **Errors** Employee not following safety or configuration management procedures.
- **Malicious damage or attacks** A disgruntled employee purposely corrupting data files.
- **Fraud** An employee falsifying travel expenses or vendor invoices and payments.
- **Theft** An employee stealing from the loading dock a laptop computer after it has been inventoried but not properly secured.
- **Equipment or software failure** An error in the calculation of a company-wide bonus overpaying employees.

Vulnerabilities are characteristics of resources that can be exploited by a threat to cause harm. Common classes of vulnerabilities include (with examples):

- **Unprotected facilities** Company offices with no security officer present or no card-entry system.
- **Unprotected computer systems** A server temporarily connected to the network before being properly configured/secured.
- **Unprotected data** Not installing critical security patches to eliminate application security vulnerabilities.
- **Insufficient procedures and controls** Allowing an accounts payable clerk to create vendors in the accounting system, enter invoices, and authorize check payments.
- **Insufficient or unqualified personnel** A junior employee not sufficiently securing a server due to a lack of training.

Step 3: Impact Determination and Quantification

An impact is the loss created when a threat exploits a vulnerability. When a threat is realized, it turns risk into impact. Impacts can be either tangible or intangible. A **tangible impact** results in financial loss or physical damage. For an **intangible impact**, assigning a financial value of the impact can be difficult. For example, in a manufacturing facility, storing and using flammable

Exam Tip: You should be able to distinguish between tangible and intangible impacts as you prepare for the Security+ exam.

chemicals creates a risk of fire to the facility. The vulnerability is that flammable chemicals are stored there. The threat would be that a person could cause a fire by mishandling the chemicals (either intentionally or unintentionally). A tangible impact would be the loss incurred (say $500,000) if a person ignites the chemicals and fire then destroys part of the facility. An example of an intangible impact would be the loss of goodwill or brand damage caused by the impression that the company doesn't safely protect its employees or the surrounding geographic area.

Tangible impacts include

- Direct loss of money
- Endangerment of staff or customers
- Loss of business opportunity
- Reduction in operational efficiency or performance
- Interruption of a business activity

Intangible impacts include

- Breach of legislation or regulatory requirements
- Loss of reputation or goodwill (brand damage)
- Breach of confidence

Tech Tip

Business Dependencies

An area often overlooked in risk assessment is the need to address business dependencies—each organization must assess risks caused by other organizations with which it interacts. This occurs when the organization is either a consumer of or a supplier to other organizations (or both). For example, if a company is dependent on products produced by a laboratory, then the company must determine the impact of the laboratory not delivering the product when needed. Likewise, an organization must assess risks that can occur when it is the supplier to some other company dependent on its products.

Step 4: Control Design and Evaluation

In this step, you determine which controls to put in place to mitigate the risks. Controls (also called countermeasures or safeguards) are designed to control risk by reducing vulnerabilities to an acceptable level. (For use in this text, the terms *control*, *countermeasure*, and *safeguard* are considered synonymous and are used interchangeably.)

Controls can be actions, devices, or procedures. They can be preventive or detective. *Preventive controls* are designed to prevent the vulnerability from causing an impact. *Detective controls* are those that detect a vulnerability that has been exploited so that action can be taken.

Exam Tip: The steps in the general risk management model should allow you to identify the steps in any risk management process.

Step 5: Residual Risk Management

Understand that risk cannot be completely eliminated. A risk that remains after implementing controls is termed a **residual risk**. In this step, you further evaluate residual risks to identify where additional controls are required to reduce risk even more. This leads us to the earlier statement that the risk management process is iterative.

Software Engineering Institute Model

In an approach tailored for managing risk in software projects, SEI uses the following paradigm (SEI, *Continuous Risk Management Guidebook* [Pittsburgh, PA: Carnegie Mellon University, 1996], 23). Although the terminology varies slightly from the previous model, the relationships are apparent, and either model can be applied wherever risk management is used.

1. **Identify**—Look for risks before they become problems.
2. **Analyze**—Convert the data gathered into information that can be used to make decisions. Evaluate the impact, probability, and timeframe of the risks. Classify and prioritize each of the risks.
3. **Plan**—Review and evaluate the risks and decide what actions to take to mitigate them. Implement those mitigating actions.
4. **Track**—Monitor the risks and the mitigation plans. Trends may provide information to activate plans and contingencies. Review periodically to measure progress and identify new risks.
5. **Control**—Make corrections for deviations from the risk mitigation plans. Correct products and processes as required. Changes in business procedures may require adjustments in plans or actions, as do faulty plans and risks that become problems.

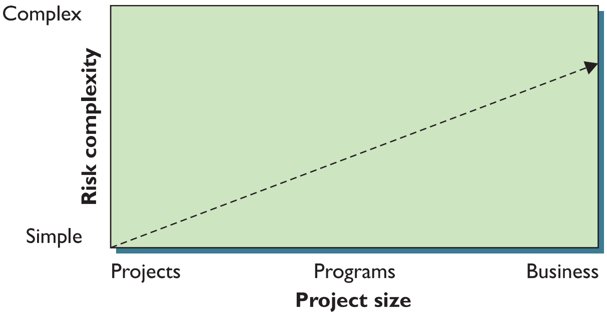
Tech Tip

Can All Risks Be Identified?

It is important to note that not all risks need to be mitigated or controlled; however, as many risks as possible should be identified and reviewed. Those deemed to have potential impact should be mitigated by countermeasures.

Model Application

The two model examples define steps that can be used in any general or software risk management process. These risk management principles can be applied to any project, program, or business activity, no matter how simple or complex. Figure 20.2 shows how risk management can be applied across the continuum and that the complexity of risk management generally increases with the size of the project, program, or business to be managed.



● Figure 20.2 Risk complexity versus project size

Qualitatively Assessing Risk

Qualitative risk analysis allows expert judgment and experience to assume a prominent role. To assess risk qualitatively, you compare the impact of the threat with the probability of occurrence and assign an impact level and probability level to the risk. For example, if a threat has a high impact and a high probability of occurring, the risk exposure is high and probably requires some action to reduce this threat (pale green box in Figure 20.3). Conversely, if the impact is low with a low probability, the risk exposure is low and no action may be required to reduce this threat (white box in Figure 20.3). Figure 20.3 shows an example of a *binary assessment*, where only two outcomes are possible each for impact and probability. Either it will have an impact or it will not (or it will have a low or high impact), and it will occur or it won't (or it will have a high probability of occurring or a low probability of occurring).

In reality, a few threats can usually be identified as presenting high-risk exposure and a few threats present low-risk exposure. The threats that fall somewhere between (pale blue boxes in Figure 20.3) will have to be evaluated by judgment and management experience.

Impact		
	High impact/Low probability	High impact/High probability
	Low impact/Low probability	Low impact/High probability
	Probability	

● Figure 20.3 Binary assessment

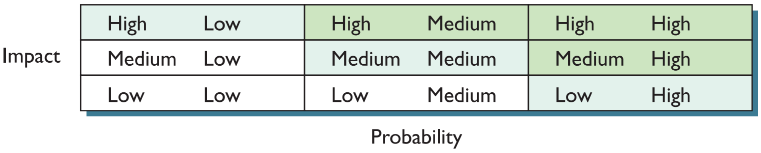
Tech Tip

System/Infrastructure KPIs

Typical KPIs for system performance include:

System KPI	***Definition***
CPU Utilization Percentage	*The percentage of CPU resources used by all the processes*
Memory Utilization Percentage	*The percentage of memory resources used by all the processes*
Busy Rate on Swap Disk	*Amount of swapping*
Daily, Weekly, and Monthly Peak Processing Times	*Periods when CPU utilization, memory utilization, and busy rate are highest*
Max, Min, and Median Run Length of Jobs	*Fastest jobs, longest-running jobs, and calculated median run length of all jobs*
Number and Name of Long-Running Jobs	*Jobs running longer than the median*
Average User Response Time	*Period of time user waits for a response after pressing the ENTER key or equivalent*

If the analysis is more complex, requiring three levels of analysis, such as low-medium-high or red-green-yellow, nine combinations are possible, as shown in Figure 20.4. Again, the pale green boxes probably require action, the white boxes may or may not require action, and the pale blue boxes require judgment. (Note that for brevity, in Figures 20.4 and 20.5, the first term in each box refers to the magnitude of the impact, and the second term refers to the probability of the threat occurring.)

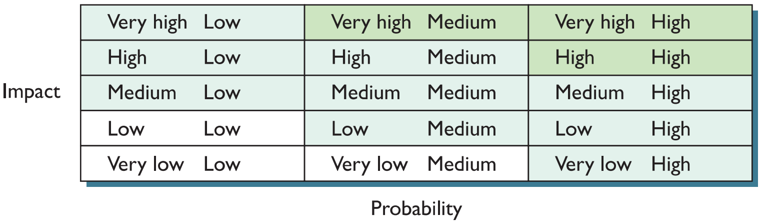


	High	Low	High	Medium	High	High
Impact	Medium	Low	Medium	Medium	Medium	High
	Low	Low	Low	Medium	Low	High

Probability

• **Figure 20.4** Three levels of analysis

Other levels of complexity are possible. With five levels of analysis, 25 values of risk exposure are possible. In this case, the possible values of impact and probability could take on the values: very low, low, medium, high, or very high. Also, note that the matrix does not have to be symmetrical. For example, if the probability is assessed with three values (low, medium, high) and the impact has five values (very low, low, medium, high, very high), the analysis would be as shown in Figure 20.5. (Again, note that the first term in each box refers to the impact, and the second term in each box refers to the probability of occurrence.)

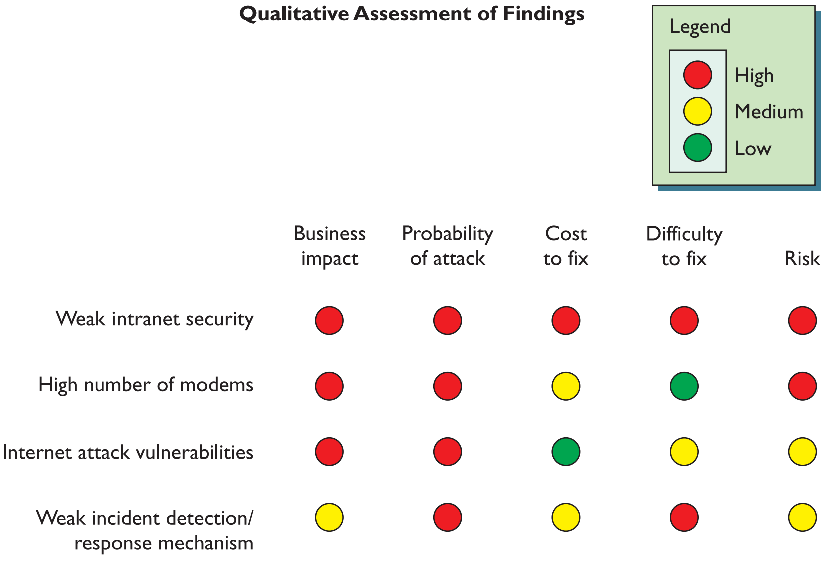


	Very high	Low	Very high	Medium	Very high	High
	High	Low	High	Medium	High	High
Impact	Medium	Low	Medium	Medium	Medium	High
	Low	Low	Low	Medium	Low	High
	Very low	Low	Very low	Medium	Very low	High

Probability

• **Figure 20.5** A 3-by-5 level analysis

So far, the examples have focused on assessing probability versus impact. Qualitative risk assessment can be adapted to a variety of attributes and situations in combination with each other. For example, Figure 20.6 shows the comparison of some specific risks that have been identified during a security assessment. The assessment identified the risk areas listed in the first column (weak intranet security, high number of modems, Internet attack vulnerabilities, and weak incident detection and response mechanisms). The assessment also identified various potential impacts listed across the top (business impact, probability of attack, cost to fix, and difficulty to fix). Each of the impacts has been assessed as low, moderate, or high—depicted using green, yellow, and red, respectively. Each of the risk areas has been assessed with respect to each of the potential impacts, and an overall risk assessment has been determined in the last column.



Qualitative Assessment of Findings

Legend

🔴	High
🟡	Medium
🟢	Low

	Business impact	Probability of attack	Cost to fix	Difficulty to fix	Risk
Weak intranet security	🔴	🔴	🔴	🔴	🔴
High number of modems	🔴	🔴	🟡	🟢	🔴
Internet attack vulnerabilities	🔴	🔴	🟢	🟡	🟡
Weak incident detection/ response mechanism	🟡	🔴	🟡	🔴	🟡

• **Figure 20.6** Example of a combination assessment

Quantitatively Assessing Risk

Whereas qualitative risk assessment relies on judgment and experience, quantitative risk assessment applies historical information and trends to attempt to predict future performance. This type of risk assessment is highly dependent on historical data, and gathering such data can be difficult. Quantitative risk assessment can also rely heavily on models that provide decision-making information in the form of quantitative metrics, which attempt to measure risk levels across a common scale.

It is important to understand that key assumptions underlie any model, and different models will produce different results even when given the same input data. Although significant research and development have been invested in improving and refining the various risk analysis models, expert judgment and experience must still be considered an essential part of any risk-assessment process. Models can never replace judgment and experience, but they can significantly enhance the decision-making process.

Adding Objectivity to a Qualitative Assessment

It is possible to move a qualitative assessment toward being more quantitative. Making a qualitative assessment more objective can be as simple as assigning numeric values to one of the tables shown in Figures 20.3 through 20.6. For example, the impacts listed in Figure 20.6 can be prioritized from highest to lowest and then weighted, as shown in Table 20.1, with business impact weighted the most and difficulty to fix weighted least.

Next, values can be assigned to reflect how each risk was assessed. Figure 20.6 can thus be made more objective by assigning a value to each color that represents an assessment. For example, a red assessment indicates

Table 20.1 Adding Weights and Definitions to the Potential Impacts

Impact	Explanation	Weight
Business impact	If exploited, would this have a material business impact?	4
Probability of attack	How likely is a potential attacker to try this technique or attack?	3
Cost to fix	How much will it cost in dollars and resources to correct this vulnerability?	2
Difficulty to fix	How hard is this to fix from a technical standpoint?	1

Table 20.2 Adding Values to Assessments

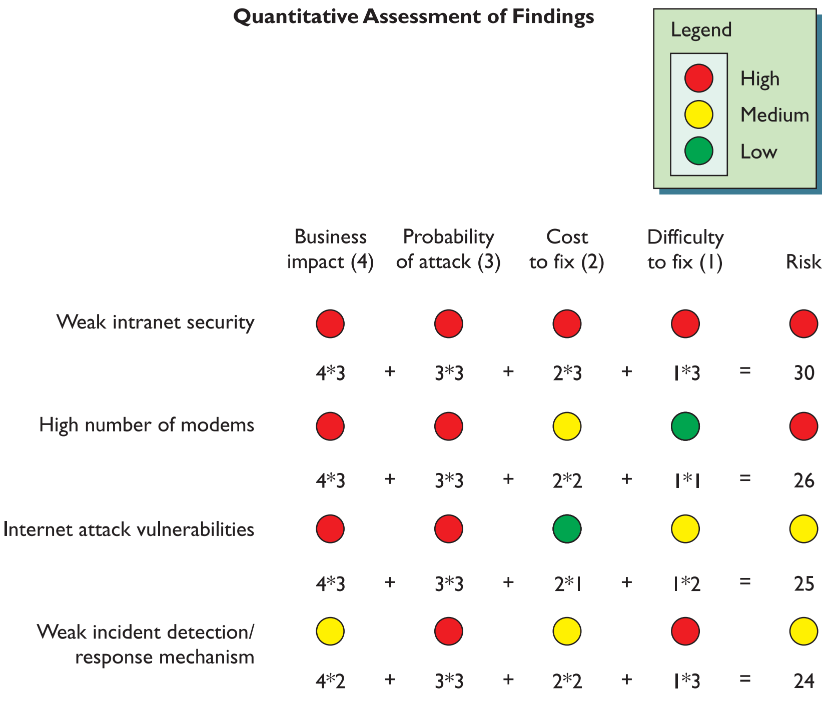
Assessment	Explanation	Value
Red	Many critical, unresolved issues	3
Yellow	Some critical, unresolved issues	2
Green	Few unresolved issues	1

many critical, unresolved issues, and this will be given an assessment value of 3. Green means few issues are unresolved, so it is given a value of 1. Table 20.2 shows values that can be assigned for an assessment using red, yellow, and green.

The last step is to calculate an overall risk value for each risk area (each row in Figure 20.6) by multiplying the weights depicted in Table 20.1 times the assessed values from Table 20.2 and summing the products:

$$\text{Risk} = W_1 * V_1 + W_2 * V_2 + \ldots W_4 * V_4$$

The risk calculation and final risk value for each risk area listed in Figure 20.6 have been incorporated into Figure 20.7. The assessed areas can then be ordered from highest to lowest based on the calculated risk value to aid management in focusing on the risk areas with the greatest potential impact.



	Business impact (4)		Probability of attack (3)		Cost to fix (2)		Difficulty to fix (1)		Risk
Weak intranet security	🔴		🔴		🔴		🔴		🔴
	4*3	+	3*3	+	2*3	+	1*3	=	30
High number of modems	🔴		🔴		🟡		🟢		🔴
	4*3	+	3*3	+	2*2	+	1*1	=	26
Internet attack vulnerabilities	🔴		🔴		🟢		🟡		🟡
	4*3	+	3*3	+	2*1	+	1*2	=	25
Weak incident detection/ response mechanism	🟡		🔴		🟡		🔴		🟡
	4*2	+	3*3	+	2*2	+	1*3	=	24

Figure 20.7 Final quantitative assessment of the findings

A Common Objective Approach

More complex models permit a variety of analyses based on statistical and mathematical models. A common method of quantitative assessment is the calculation of the annualized loss expectancy (ALE). Calculating the ALE creates a monetary value of the impact. This calculation begins by calculating a single loss expectancy (SLE) with the following formula:

$$\text{SLE} = \textit{asset value} * \textit{exposure factor}$$

By example, to calculate the exposure factor, assume the asset value of a small office building and its contents is $2 million. Also assume that this building houses the call center for a business, and the complete loss of the center would take away about half of the capability of the company. Therefore, the exposure factor is 50 percent. The SLE is

$2 million * 0.5 = $1 million

The ALE is then calculated simply by multiplying the SLE by the likelihood or number of times the event is expected to occur in a year, which is called the annualized rate of occurrence (ARO):

ALE = SLE * ARO

If the event is expected to occur once in 20 years, then the ARO is 1/20. Typically the ARO is defined by historical data, either from a company's own experience or from industry surveys. Continuing our example, assume that a fire at this business's location is expected to occur about once in 20 years. Given this information, the ALE is

$1 million * 1/20 = $50,000

The ALE determines a threshold for evaluating the cost/benefit ratio of a given countermeasure. Therefore, a countermeasure to protect this business adequately should cost no more than the calculated ALE of $50,000 per year.

The examples in this chapter have been simplistic, but they demonstrate the concepts of both qualitative and quantitative risk analysis. More complex algorithms and software packages are available for accomplishing risk analyses, but these examples suffice for the purposes of this text.

Tech Tip

Resources for Calculating ALE

Numerous resources are available to help in calculating ALE. For example, http://rm.iso.com/Capabilities/Capabilities/Data.html has databases that contain information to help businesses (member institutions) manage exposure to loss from natural disasters such as hurricanes, earthquakes, and so forth. There is information on property perils such as fire, lightning, vandalism, windstorm, hail, and so forth. It even includes information to help evaluate the effectiveness of your building's sprinkler systems.

Try This

Calculate SLE, ARO, and ALE

A company owns five warehouses throughout the United States, each of which is valued at $1 million and contributes equally to the company's capacity. Try calculating the SLE, ARO, and ALE for its warehouse located in the Mountain West, where the probability of an earthquake is once every 500 years. The solution is given in the footnote immediately below.[1]

[1] SLE = $1 million * 1.0; ARO = 1/500; ALE = $1 million/500, or $2000.

Exam Tip: It is always advisable to memorize these fundamental equations for certifications such as Security+.

Qualitative vs. Quantitative Risk Assessment

It is recognized throughout industry that it is *impossible* to conduct risk management that is purely *quantitative*. Usually risk management includes both qualitative and quantitative elements, requiring both analysis and judgment or experience. In contrast to quantitative assessment, it is *possible* to accomplish *purely qualitative* risk management. It is easy to see that it is impossible to define and quantitatively measure all factors that exist in a given risk assessment. It is also easy to see that a risk assessment that measures no factors quantitatively but measures them all qualitatively is possible.

The decision of whether to use qualitative versus quantitative risk management depends on the criticality of the project, the resources available, and the management style. The decision will be influenced by the degree to which the fundamental risk management metrics, such as asset value, exposure factor, and threat frequency, can be quantitatively defined.

Tools

Many tools can be used to enhance the risk management process. The following tools can be used during the various phases of risk assessment to add objectivity and structure to the process. Understanding the details of each of these tools is not necessary for the Security+ exam, but understanding what they can be used for is important. More information on these tools can be found in any good project-management text.

- **Affinity grouping** A method of identifying items that are related and then identifying the principle that ties them together.
- **Baseline identification and analysis** The process of establishing a baseline set of risks. It produces a "snapshot" of all the identified risks at a given point in time.
- **Cause and effect analysis** Identifying relationships between a risk and the factors that can cause it. This is usually accomplished using *fishbone diagrams* developed by Dr. Kaoru Ishikawa, former professor of engineering at the Science University of Tokyo.
- **Cost/benefit analysis** A straightforward method for comparing cost estimates with the benefits of a mitigation strategy.
- **Gantt charts** A management tool for diagramming schedules, events, and activity duration.
- **Interrelationship digraphs** A method for identifying cause-and-effect relationships by clearly defining the problem to be solved, identifying the key elements of the problem, and then describing the relationships between each of the key elements.
- **Pareto charts** A histogram that ranks the categories in a chart from most frequent to least frequent, thus facilitating risk prioritization.
- **PERT (program evaluation and review technique) charts** A diagram depicting interdependencies between project activities, showing the sequence and duration of each activity. When complete, the chart shows the time necessary to complete the project and the activities that determine that time (the critical path). The earliest and latest start and stop times for each activity and available slack times can also be shown.
- **Risk management plan** A comprehensive plan documenting how risks will be managed on a given project. It contains processes, activities, milestones, organizations, responsibilities, and details of each major risk management activity and how it is to be accomplished. It is an integral part of the project management plan.

Tech Tip

Accepting Risk

In addition to mitigating risk or transferring risk, it may be acceptable for a manager to accept risk in that despite the potential cost of a given risk and its associated probability, the manager of the organization will accept responsibility for the risk if it does happen. For example, a manager may choose to allow a programmer to make "emergency" changes to a production system (in violation of good segregation of duties) because the system cannot go down during a given period of time. The manager accepts the risk that the programmer could possibly make unauthorized changes because of the high-availability requirement of that system. However, there should always be some additional controls such as a management review or a standardized approval process to ensure the assumed risk is adequately managed.

Tech Tip

Risks Really Don't Change, But They Can Be Mitigated

One final thought to keep in mind is that the risk itself doesn't really change, no matter what actions are taken to mitigate that risk. A high risk will always be a high risk. However, actions can be taken to reduce the impact of that risk if it occurs.

Chapter 20 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following about risk management.

Use risk management tools and principles to manage risk effectively

- Risk management is a key management process that must be used at every level, whether managing a project, a program, or an enterprise.
- Risk management is also a strategic tool to more effectively manage increasingly sophisticated, diverse, and geographically expansive business opportunities.
- Managing risk is key to keeping a business competitive and must be done by managers at all levels.
- Common business risks include fraud and management of treasury, revenue, contracts, environment, regulatory issues, business continuity, and technology.
- Technology is a business risk that is so important it must be specifically managed.
- Technology risks include security and privacy, information technology operations, business systems control and effectiveness, information systems testing, and management of business continuity, reliability and performance, information technology assets, project risk, and change.
- A general model for managing risk includes asset identification, threat assessment, impact definition and quantification, control design and evaluation, and residual risk management.
- The SEI model for managing risk includes these steps: identify, analyze, plan, track, and control.

Explain the differences between qualitative and quantitative risk assessment

- Both qualitative and quantitative risk assessment approaches must be used to manage risk effectively, and a number of approaches were presented in this chapter.
- Qualitative risk assessment relies on expert judgment and experience by comparing the impact of a threat with the probability of it occurring.
- Qualitative risk assessment can be a simple binary assessment weighing high or low impact against high or low probability. Additional levels can be used to increase the comprehensiveness of the analysis. The well-known red-yellow-green stoplight mechanism is qualitative in nature and is easily understood.
- Quantitative risk assessment applies historical information and trends to assess risk. Models are often used to provide information to decision-makers.
- A common quantitative approach calculates the annualized loss expectancy from the single loss expectancy and the annualized rate of occurrence (ALE = SLE * ARO).
- It is important to understand that it is impossible to conduct a purely quantitative risk assessment, but it is possible to conduct a purely qualitative risk assessment.

Describe essential risk management tools

- Numerous tools can be used to add credibility and rigor to the risk assessment process.
- Risk assessment tools help identify relationships, causes, and effects. They assist in prioritizing decisions and facilitate effective management of the risk management process.

Key Terms

annualized loss expectancy (ALE) *(539)*
annualized rate of occurrence (ARO) *(539)*
asset *(538)*
control *(538)*
countermeasure *(538)*
exposure factor *(539)*

impact *(538)*
intangible impact *(543)*
mitigate *(539)*
qualitative risk assessment *(538)*
quantitative risk assessment *(539)*
residual risk *(544)*
risk *(538)*
risk analysis *(538)*
risk assessment *(538)*
risk management *(538)*
safeguard *(538)*
single loss expectancy (SLE) *(539)*
tangible impact *(543)*
threat *(538)*
vulnerability *(538)*

Key Terms Quiz

Use terms from the Key Terms list to complete the sentences that follow. Don't use the same term more than once. Not all terms will be used.

1. Asset value * exposure factor = _______________.
2. A control may also be called a(n) _______________ or a(n) _______________.
3. When a threat exploits a vulnerability, you experience a(n) _______________.
4. Single loss expectancy * annualized rate of occurrence = _______________.
5. If you reduce the likelihood of a threat occurring, you _______________ a risk.
6. The _______________ measures the magnitude of the loss of an asset.
7. Risk analysis is synonymous with _______________.
8. Any circumstance or event with the potential to cause harm to an asset is a(n) _______________.
9. A characteristic of an asset that can be exploited by a threat to cause harm is its _______________.
10. _______________ is the overall decision-making process of identifying threats and vulnerabilities and their potential impacts, determining the costs to mitigate such events, and deciding what cost-effective actions need to be taken to control these risks.

Multiple-Choice Quiz

1. Which of the following correctly defines qualitative risk management?
   - **A.** The process of objectively determining the impact of an event that affects a project, program, or business.
   - **B.** The process of subjectively determining the impact of an event that affects a project, program, or business.
   - **C.** The loss that results when a vulnerability is exploited by a threat.
   - **D.** To reduce the likelihood of a threat occurring.
2. Which of the following correctly defines risk?
   - **A.** The risks still remaining after an iteration of risk management.
   - **B.** The loss that results when a vulnerability is exploited by a threat.
   - **C.** Any circumstance or event with the potential to cause harm to an asset.
   - **D.** The possibility of suffering harm or loss.
3. Single loss expectancy (SLE) can best be defined by which of the following equations?
   - **A.** SLE = annualized loss expectancy * annualized rate of occurrence
   - **B.** SLE = asset value * exposure factor
   - **C.** SLE = asset value * annualized rate of occurrence
   - **D.** SLE = annualized loss expectancy * exposure factor
4. Which of the following correctly defines annualized rate of occurrence?
   - **A.** How much an event is expected to cost per year

B. A measure of the magnitude of loss of an asset

C. On an annualized basis, the frequency with which an event is expected to occur

D. The resources or information an organization needs to conduct its business

5. Which of the following is a technology risk?

A. Business continuity management

B. Fraud

C. Contract management

D. Treasury management

6. The Basel Committee defines operational risk as which of the following?

A. Risk from disruption by people, systems, processes, or disasters

B. Risk of default of outstanding loans

C. Risk of losses due to fluctuations of market prices

D. The possibility of suffering harm or loss

7. Which of the following is *not* an asset?

A. Equipment failure

B. Hardware

C. Inventory

D. Cash

For questions 8 and 9, assume the following: The asset value of a small distribution warehouse is $5 million, and this warehouse serves as a backup facility. Its complete destruction by a disaster would take away about 1/5 of the capability of the business. Also assume that this sort of disaster is expected to occur about once every 50 years.

8. Which of the following is the calculated single loss expectancy (SLE)?

A. SLE = $25 million

B. SLE = $1 million

C. SLE = $2.5 million

D. SLE = $5 million

9. Which of the following is the calculated annualized loss expectancy (ALE)?

A. ALE = $50,000

B. ALE = $1 million

C. ALE = $20,000

D. ALE = $50 million

10. When discussing qualitative risk assessment versus quantitative risk assessment, which of the following is true?

A. It is impossible to conduct a purely quantitative risk assessment, and it is impossible to conduct a purely qualitative risk assessment.

B. It is possible to conduct a purely quantitative risk assessment, but it is impossible to conduct a purely qualitative risk assessment.

C. It is impossible to conduct a purely quantitative risk assessment, but it is possible to conduct a purely qualitative risk assessment.

D. It is possible to conduct a purely quantitative risk assessment, and it is possible to conduct a purely qualitative risk assessment.

11. Which of the following correctly defines residual risk?

A. The risks still remaining after an iteration of risk management

B. The possibility of suffering a loss

C. The result of a vulnerability being exploited by a threat that results in a loss

D. Characteristics of an asset that can be exploited by a threat to cause harm

12. Which of the following is a business risk?

A. Change management

B. Security and privacy

C. Environmental risk management

D. Business continuity management

13. Which of the following statements about risk is true?

A. A manager can accept the risk, which will reduce the risk.

B. The risk itself doesn't really change. However, actions can be taken to reduce the impact of the risk.

C. A manager can transfer the risk, which will reduce the risk.

D. A manager can take steps to increase the risk.

14. Which of the following correctly defines a Gantt chart?

A. A method of identifying items that are related and then identifying the principle that ties them together into a group

B. A management tool for diagramming schedules, events, and activity duration

C. A single-page form used to document new risks as they occur

D. A diagram depicting interdependencies between project activities, showing the sequence and duration of each activity

15. Which of the following is *not* a viable option when dealing with risk?

A. A manager can take action to mitigate risk.

B. A manager can take action to transfer risk.

C. A manager can take action to increase risk.

D. A manager can take action to accept risk.

Essay Quiz

1. You are drafting an e-mail to your risk management team members to explain the difference between tangible assets and intangible assets. Relate to tangible and intangible impacts. Write a one- or two-sentence paragraph that explains the difference and include two examples of each.

2. You have been tasked to initiate a risk management program for your company. The CEO has just asked you to succinctly explain the relationship between impact, threat, and vulnerability. Think quick on your feet and state a single sentence that explains the relationship.

3. Your CEO now says, "You mentioned that risks always exist. If I take enough measures, can't I eliminate the risk?" Explain why risks always exist.

4. You are explaining your risk management plan to a new team member just brought on as part of a college internship program. The intern asks, "With respect to impact, what does a threat do to a risk?" How would you answer?

5. The intern mentioned in Question 4 now asks you to compare and contrast accepting risk, transferring risk, and mitigating risk. What's your response?

Lab Projects

• Lab Project 20.1

The asset value of a distribution center (located in the midwestern United States) and its inventory is $10 million. It is one of two identical facilities (the other is in the southwestern United States). Its complete destruction by a disaster would thus take away half of the capability of the business. Also assume that this sort of disaster is expected to occur about once every 100 years. From this, calculate the annualized loss expectancy.

• Lab Project 20.2

You have just completed a qualitative threat assessment of the computer security of your organization, with the impacts and probabilities of occurrence listed in the table that follows. Properly place the threats in a 3-by-3 table similar to that in Figure 20.4. Which of the threats should you take action on, which should you monitor, and which ones may not need your immediate attention?

Threat	Impact	Probability of Occurrence
Virus attacks	High	High
Internet hacks	Medium	High
Wireless hacks	Low	High
Disgruntled employee hacks	High	Medium
Weak incidence response mechanisms	Medium	Medium
Theft of information by a trusted third-party contractor	Low	Medium
Competitor hacks	High	Low
Dial-up hacks	Medium	Low
Inadvertent release of noncritical information	Low	Low