CHAPTER 8 Risk Management

LEARNING OUTCOMES

By the end of this chapter, you should be able to:

1. Identify the risk and the risk impact;
2. Explain the purpose of risk management;
3. Describe an approach to effectively manage risk;
4. Determine the qualitative and quantitative risk assessment; and
5. Describe various tools related to risk management;

INTRODUCTION

Look at the diagram given below.

What do you understand from the diagram above? The diagram shows the risk management process. Based from the diagram given, provide a situation, base on your understanding and the key points provided on risk management. Share your research in the LMS Forum.

Risk management can best be described as a decision making process. In the simplest term, when you manage risk, you determine what could happen to your business, you access 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 can then decide to act or not to act and finally evaluate the results of your decision. The process may then iterate.

Industry best practices clearly indicate that an important aspect of effectively managing risk is to consider it an ongoing process. Effective risk management avoids costly over-sights and unexpected problems.

8.1 RISK MANAGEMENT CONCEPT

A risk is a potential problem that the system or its users may experience. It normally refers to something that is "uncertain" and that uncertainty normally carries a loss or adverse effect.

According to Webster's dictionary, risk is "the possibility of loss or injury also the degree of the probability of such loss".

There are four components of risk as shown in Figure 8.1.

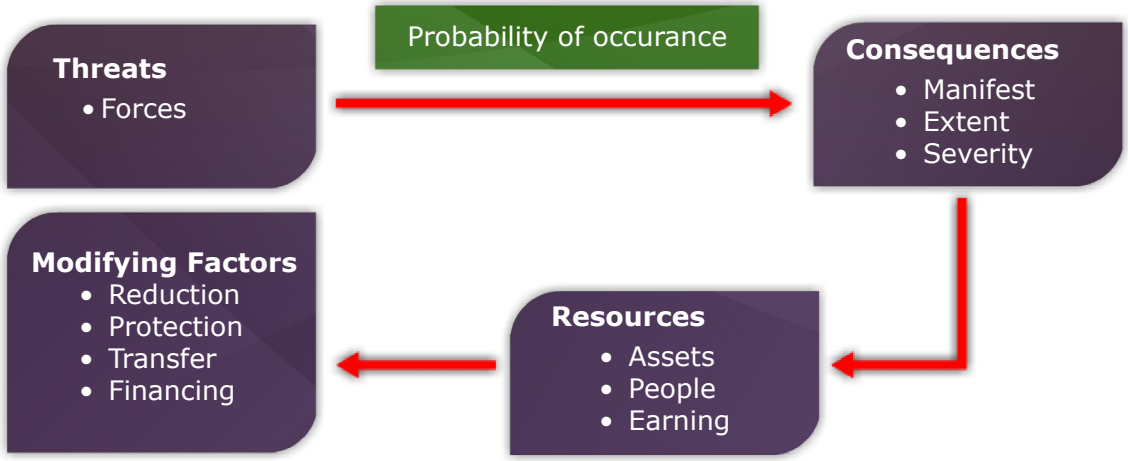


Figure 8.1: The four risk components

From Figure 8.1, let us look at each of the risk components below.

1. Threats

Threats are the broad range of forces capability of producing adverse consequences.

2. Resources

Resources consist of the assets, people or earning potentially affected by threats.

3. Modifying factors

Modifying factors are the internal and external factors that influence the probability of a threat becoming a reality or the severity of consequences when the threat materialises.

4. Consequences

Consequences have to do with the way the threat manifests its effects upon the resources

and the extent of those effects.

> ***Risk management*** is the science and art recognising the existence of threats, determining their consequences to resources and applying modifying factors in a cost-effective manner to keep adverse consequences within bounds.

It is an essential element of management from the enterprise level down to the individual project. It compasses all the actions taken to reduce complexity, increase objectivity and identify important decision factors.

Business must take risks to retain their competitive edge. Thus, a result, risk management must be done as part of managing any business, any program or any project to protect the business from possible negative occurrences, as well as recognise opportunities and capitalise on all possible threats or security problems when they arise.

Therefore, risk management concept emphasises on the systematic identification, analysis and assessment of all hazards inherent in an activity so that effective measures can be established to control the risks. Without an understanding of what needs to be control, it will be difficult for the management to take the right actions to the problems.

In short, risk management is the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

Risk assessment and risk analysis involve a methodological investigation of the organisation's resources, personnel, procedures and objectives to determine points of weakness. Finding each point, organisations overtly manage the risk by strengthening the weak points or passing the risk to someone else.

8.1.1 Types of Risk

Every risk has its own distinct characteristic that requires particular management or analysis. Most people will recognise the 'obvious', or most apparent, risk that they are facing.

An emerging concept in risk management is that there are three types of risk as depicted in Figure 8.2.

Figure 8.2: Types of risk and their management

Opportunity-based Risk

There are two main aspects of opportunity-based risks:

- Risks associated with not taking an opportunity; and
- Those associated with taking an opportunity.

The latter is a conscious decision to accept identified risk associated with an opportunity and then to implement processes to minimise any negative impacts and maximise gains. Opportunity-based risk may or may not be visible or physically apparent; it is often financial; it can have a positive or negative outcome; and it can have both short-term and longer-term outcomes.

Uncertainty-based Risk

Uncertainty-based risk is the risk associated with unknown and unexpected events. This type of risk has attracted more recognition as a result of events such as Y2K, September 11 and recent natural disasters such as the Asian tsunami.

Uncertainty-based risks are:

- Unknown or extremely difficult to quantify;

- Catastrophic or disastrous in nature;
- Associated with negative outcomes; and
- Not possible to control or influence.

Uncertainty-based risks for small business include:

- Physical damage or damage to buildings by fire or flood;
- Financial loss;
- Loss of a vital supplier; unexpected loss of insurance; and
- Loss of market share.

Preparing for uncertainty

By their very nature, disaster and the unexpected are unpredictable. A business owner must plan accordingly and determine how to minimise business disruption.

There are various management methods to minimise the impact of uncertain events on a business. For examples, disaster and emergency planning, planning to recover from a disaster and business continuity planning to ensure a business can continue to operate after a major disruption.

Hazard-based Risk

Hazard-based risk is the risk associated with a source of potential harm or a situation with the potential to cause harm.

The types of hazard-based risks can be well described in Table 8.1.

Table 8.1: The Types of Hazard

Hazard-based Risks	Descriptions
Physical hazards	This includes noise, temperature or other environmental factors.
Chemical hazards	This includes storage and/or use of flammable, poisonous, toxic or carcinogenic chemicals.
Physical hazards	This includes viruses, bacteria, fungi and other hazardous organisms.
Ergonomic hazards	This includes poor workspace design, layout or activity and equipment usage.

8.1.2 Risk Management Model

Risk management concepts are fundamentally the same despite their definitions, requiring similar skills, tools and methodologies. There are several models for managing risk through its various phases. The model you choose should align with your business objectives and strategies.

There are two risk management models that can be used. These two risk management models are well described in Figure 8.3.

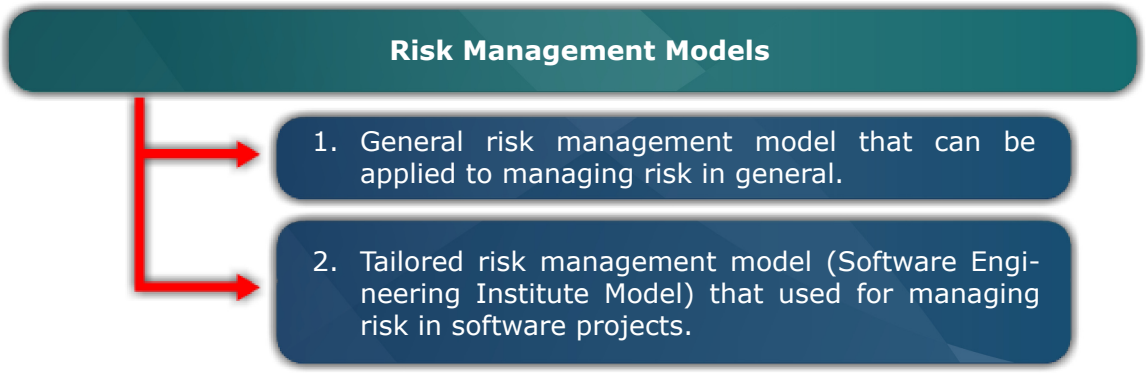


Figure 8.3: The two types of risk management models

8.1.2.1 General Risk Management Model

This model can be applied for managing the risk in general. A general model for managing risk includes asset identification, threat assessment, impact definition and quantification, control design and evaluation, and residual risk management.

1. Assets Identification

In this step, assets, systems and processes that need protection is identified and classified because they are vulnerable to threats. This classification leads to the ability to prioritise assets, systems and processes and to evaluate the costs of addressing the associated risks. A monetary value can be determined for tangible assets whereas a monetary value cannot be determined for intangible assets.

Assets can include inventory, buildings, cash, information and data, hardware, software, services, documents, personnel, brand recognition, organisation reputation and goodwill.

2. Threats Assessment

This step identifies the possible threats and vulnerabilities associated with each asset the likelihood of their occurrence. Threats can be defined as any circumstance

or event with the potential to cause harm to an asset. The common classes of threats include natural disasters, man-made disasters, terrorism, errors, malicious damage or attacks, fraud, theft and equipment or software failure.

Vulnerabilities are characteristics of resources that can be exploited by a threat to cause harm. Examples of vulnerabilities are as shown in Figure 8.4.

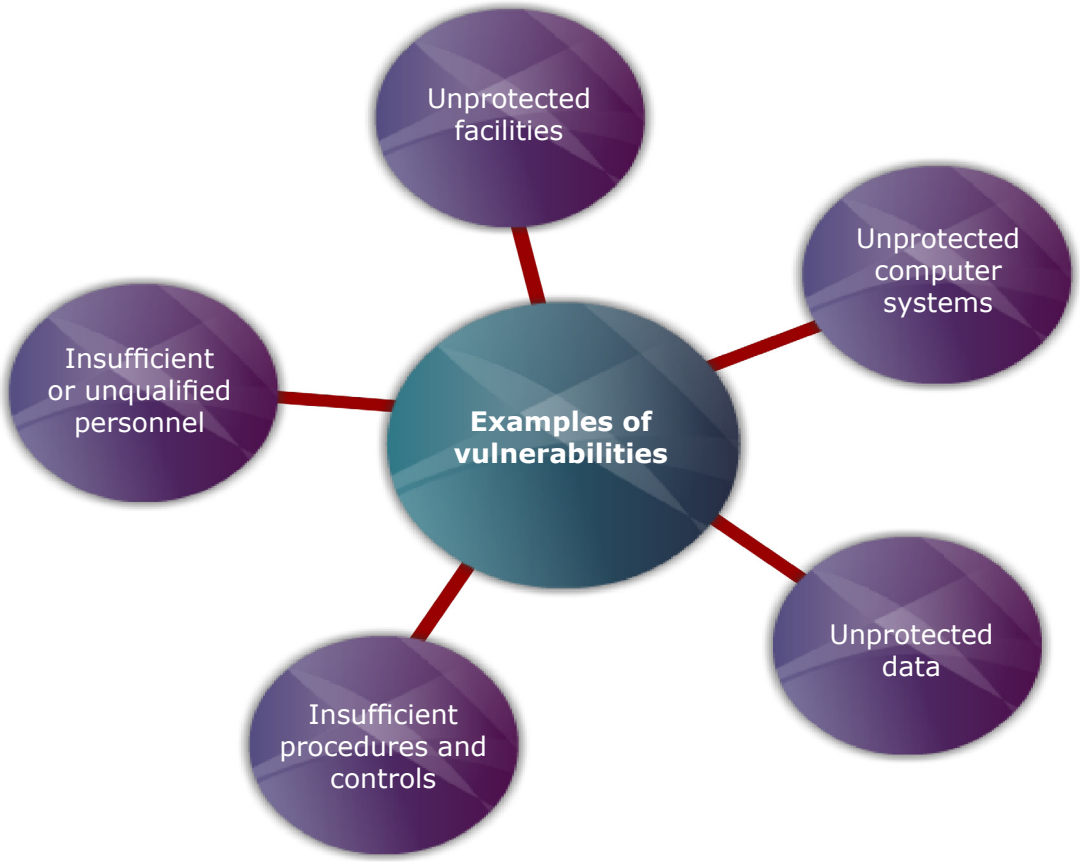


Figure 8.4: Examples of vulnerabilities

3. Impact Definition and Quantification

An impact is the loss created when a threat exploits vulnerability. When a threat is realised, it turns risk into impact. Impacts can be either tangible or intangible. Tangible impacts include direct loss of money, endangerment of staff or customers, loss of business opportunity, reduction in operational efficiency or performance, and interruption of a business activity. The intangible impacts include breach of legislation or regulatory requirements, loss of reputation or goodwill (brand damage), and breach of confidence.

4. Control Design and Evaluation

Controls that also called as countermeasures or safeguards are designed to control

risk by reducing vulnerabilities to an acceptable level. It can be actions, devices or procedures that can be preventive or detective.

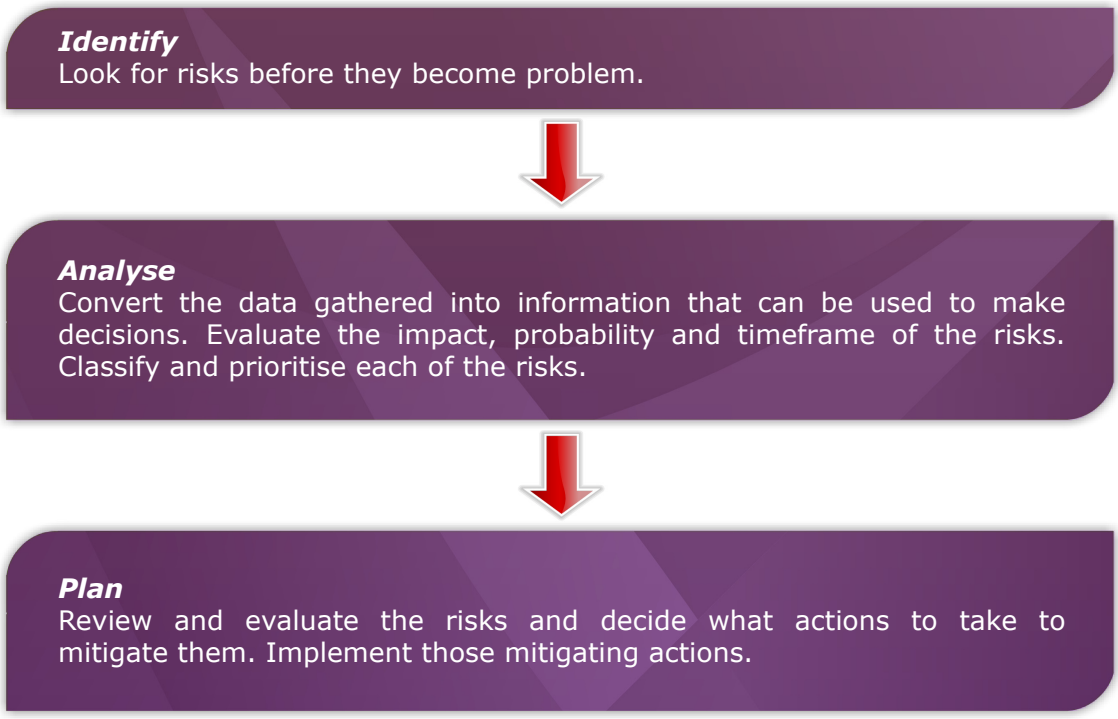
Preventive controls are designed to prevent the vulnerability from being exploited by a threat thus causing an impact. Detective controls are those that detect a vulnerability that has been exploited by a threat so that action can be taken.

5. Residual Risk Management

It is important to understand that risk cannot be residual risk. Any risks that remain after implementing controls are termed residual risks. Residual risk can be further evaluated 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. Business process reengineering or organisational changes can create new risks or weaken existing control activities.

8.1.2.2 Software Engineering Institute Model

Although the terminology varies slightly from the general risk management model, the relationships are apparent and either model can be applied wherever risk management is used. The SEI model for managing risk involves these steps as displayed in Figure 8.5.



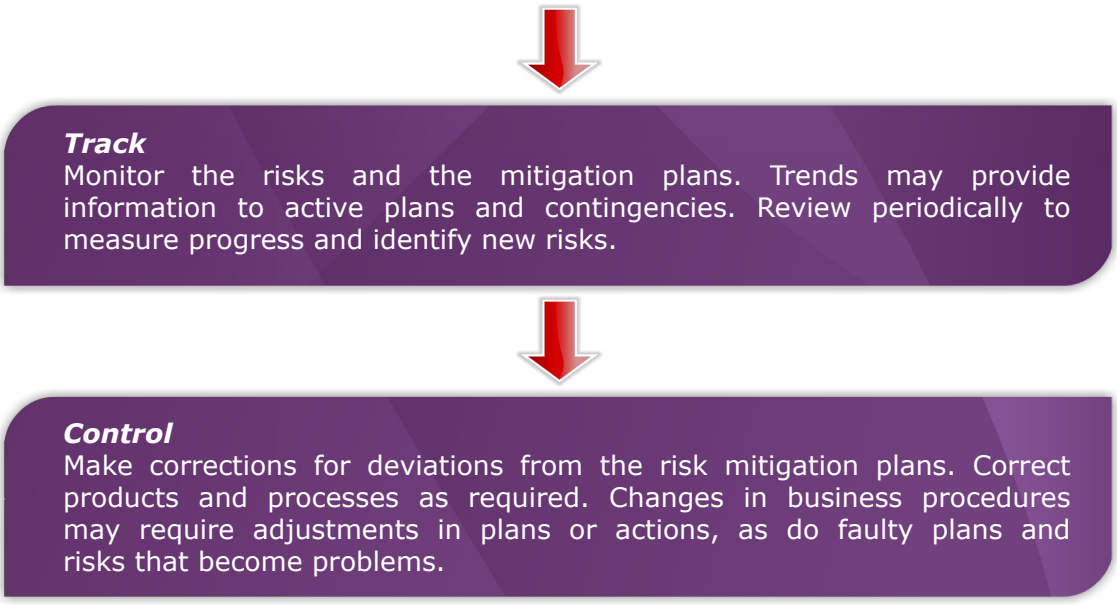


Figure 8.5: The steps in SEI model for managing risk

These two models 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.

8.1.3 Risk Assessment

A ***risk assessment*** involves evaluating existing security and controls and assessing their adequacy relative to the potential threats of the organisation.

Risk assessment often produces an important side benefit that is in-depth knowledge about a system and an organisation as risk analysts try to figure out how systems and functions are interrelated.

A risk assessment can focus on many different areas such as: technical and operational controls to be designed into a new application, the use of telecommunications, a data center, or an entire organisation.

8.1.3.1 Types of Risk Assessment

There are a number of distinct approaches to risk assessment. However, these essentially break down into two types (see Figure 8.6).

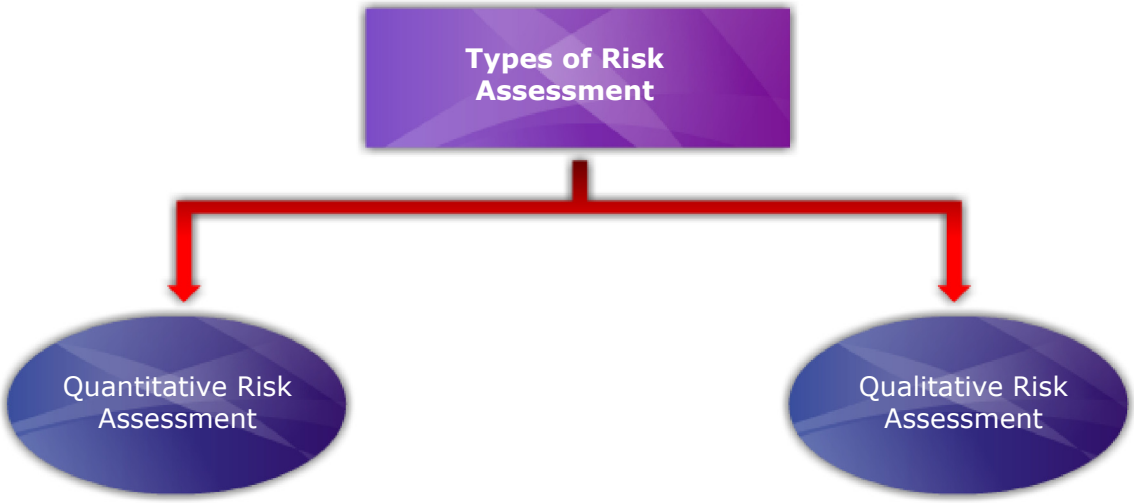


Figure 8.6: The two types of risk assessment

From Figure 8.6, let us look in details each of the risk assessment types.

Quantitative Risk Assessment

Quantitative risk assessment applies historical information and trends to assess risk. Models are often used to provide information decision-makers. Quantitative risk assessment makes use of a single figure produced from these elements. This is called the ***Annual Loss Expectancy (ALE)*** or the ***Estimated Annual Cost (EAC)***. This is calculated for an event by simply multiplying the potential loss by the probability. It is thus theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this.

The problems with this type of risk assessment are usually associated with the unreliability and inaccuracy of the data. Probability can rarely be precise and can, in some cases, promote complacency. In addition, controls and countermeasures often tackle a number of potential events and the events themselves are frequently interrelated.

Qualitative Risk Assessment

Qualitative risk assessment relies on expert judgment and experience by comparing the impact of a threat with the probability of it occurring. This is by far the most widely used approach to risk assessment. Probability data is not required and only estimated potential loss is used. Most qualitative risk assessment methodologies make use of a number of interrelated elements that are shown in Table 8.2.

Table 8.2: Interrelated Elements in Qualitative Risk Assessment

Qualitative Risk Assessment	Descriptions
Physical hazards	These are things that can go wrong or that can attack the system. Examples might include fire or fraud. Threats are ever present for every system.
Vulnerabilities	These make a system more prone to attack by a threat or make an attack more likely to have some success or impact.
Controls	These are the countermeasures for vulnerabilities. There are four types which are *deterrent controls* that reduce the likelihood of a deliberate attack, *preventative controls* that protect vulnerabilities and make an attack unsuccessful or reduce its impact, *corrective controls* that reduce the effect of an attack, and *detective controls* that discover attacks and trigger preventative or corrective controls.

These elements can be illustrated by a simple relational model as in Figure 8.7.

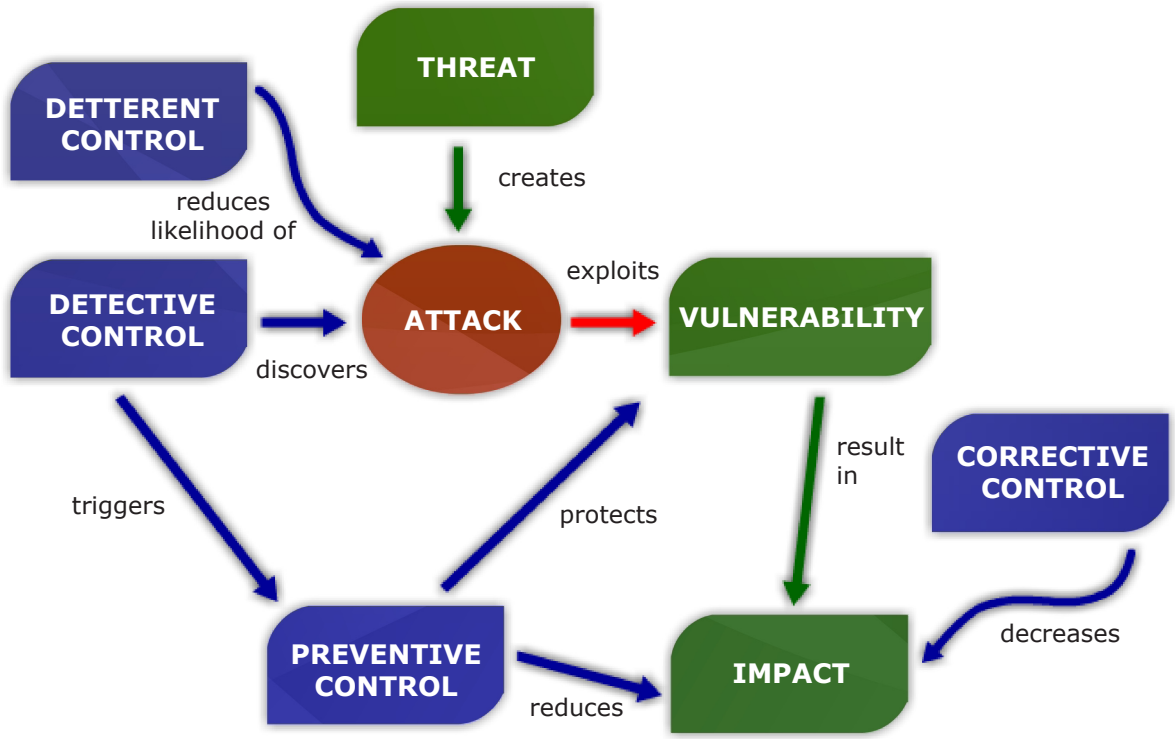


Figure 8.7: Elements of qualitative risk assessment relationships

However, recognised throughout industry that is impossible to conduct risk management that is purely quantitative. Thus, both qualitative and quantitative risk assessment approaches must be used to effectively manage risk.

8.1.3.2 Basic Risk Assessment Activities

Risk assessment, the process of analysing and interpreting risk, is comprised of three basic steps of activities that are shown in Figure 8.8.

Figure 8.8: The three basic steps of activities in risk management

1. Determining the Assessment's Scope and Methodology

The first step in assessing risk is to identify the system under consideration, the part of the system that will be analysed, and the analytical method including its level of detail and formality.

The assessment may be focused on certain areas where either the degree of risk is unknown or is known to be high. Different parts of a system may be analysed in greater or lesser detail. Defining the scope and boundary can help ensure a cost-effective assessment.

Factors that influence scope include:

- What phase of the life cycle a system is in - more detail might be appropriate for a new system being developed than for an existing system undergoing an upgrade;
- The relative importance of the system under examination - the more essential the system, the more thorough the risk analysis should be; and

- The magnitude and types of changes the system has undergone since the last risk analysis. The addition of new interfaces would warrant a different scope than would install a new operating system.

Methodologies can be formal or informal, detailed or simplified, high or low level, quantitative (computationally based) or qualitative (based on descriptions or rankings), or a combination of these. No single method is best for all users and all environments.

How the boundary, scope, and methodology are defined will have major consequences in terms of the total amount of effort spent on risk management and the type and usefulness of the assessment's results. The boundary and scope should be selected in a way that will produce an outcome that is clear, specific, and useful to the system and environment under scrutiny.

2. Collecting and Analysing Data

Risk has many different components such as assets, threats, vulnerabilities, safeguards, consequences, and likelihood. This examination normally includes gathering data about the threatened area and synthesizing and analysing the information to make it useful.

Because it is possible to collect much more information than can be analysed, steps need to be taken to limit information gathering and analysis. This process is called screening. A risk management effort should focus on those areas that result in the greatest consequence to the organisation that can cause the most harm. This can be done by ranking threats and assets.

A risk management methodology does not necessarily need to analyse each of the components of risk separately (see Table 8.3). For example, assets/consequences or threats/likelihoods may be analysed together.

Table 8.3: The Risk Management Methodology

Risk Management	Descriptions
Asset Valuation	• These include the information, software, personnel, hardware and physical assets (such as the computer facility). • The value of an asset consists of its intrinsic value and the near-term impacts and long-term consequences of its compromise.

Consequence Assessment	• The consequence assessment estimates the degree of harm or loss that could occur. • Consequences refer to the overall, aggregate harm that occurs, not just to the nearterm or immediate impacts. • While such impacts often result in disclosure, modification, destruction or denial of service, consequences are the more significant long-term effects, such as lost business, failure to perform the system's mission, loss of reputation, violation of privacy, injury or loss of life. • The more severe the consequences of a threat, the greater the risk to the system or the organisation.
Threat Identification	• A threat is an entity or event with the potential to harm the system. • Typical threats are errors, fraud, disgruntled employees, fires, water damage, hackers and viruses. • Threats should be identified and analysed to determine the likelihood of their occurrence and their potential to harm assets.
Safeguard Analysis	• A safeguard is any action, device, procedure, technique, or other measure that reduces a system's vulnerability to a threat. • Safeguard analysis should include an examination of the effectiveness of the existing security mea-sures. • It can also identify new safeguards that could be implemented in the system. • However, this is normally performed later in the risk management process.
Vulnerability Analysis	• A vulnerability is a condition or weakness in or absence of security procedures, technical controls, physical controls or other controls that could be exploited by a threat. • Vulnerabilities are often analysed in terms of missing safeguards.

	• Vulnerabilities contribute to risk because they may "allow" a threat to harm the system. • The interrelationship of vulnerabilities, threats and assets is critical to the analysis of risk. • Some of these interrelationships are pictured in Figure 8.4. • However, there are other interrelationships such as the presence of a vulnerability inducing a threat. (For example, a normally honest employee might be tempted to alter data when the employee sees that a terminal has been left logged on).
Likelihood Assessment	• Likelihood is an estimation of the frequency or chance of a threat happening. • A likelihood assessment considers the presence, tenacity and strengths of threats as well as the effectiveness of safeguards (or presence of vulnerabilities). • In general, historical information about many threats is weak, particularly with regard to human threats; thus, experience in this area is important. • Some threat data especially on physical threats such as fires or floods is stronger. • Care needs to be taken in using any statistical threat data; the source of the data or the analysis may be inaccurate or incomplete. • In general, the greater the likelihood of a threat occurring, the greater the risk.

Figure 8.9 shows the interrelationship vulnerabilities, threats and assets.

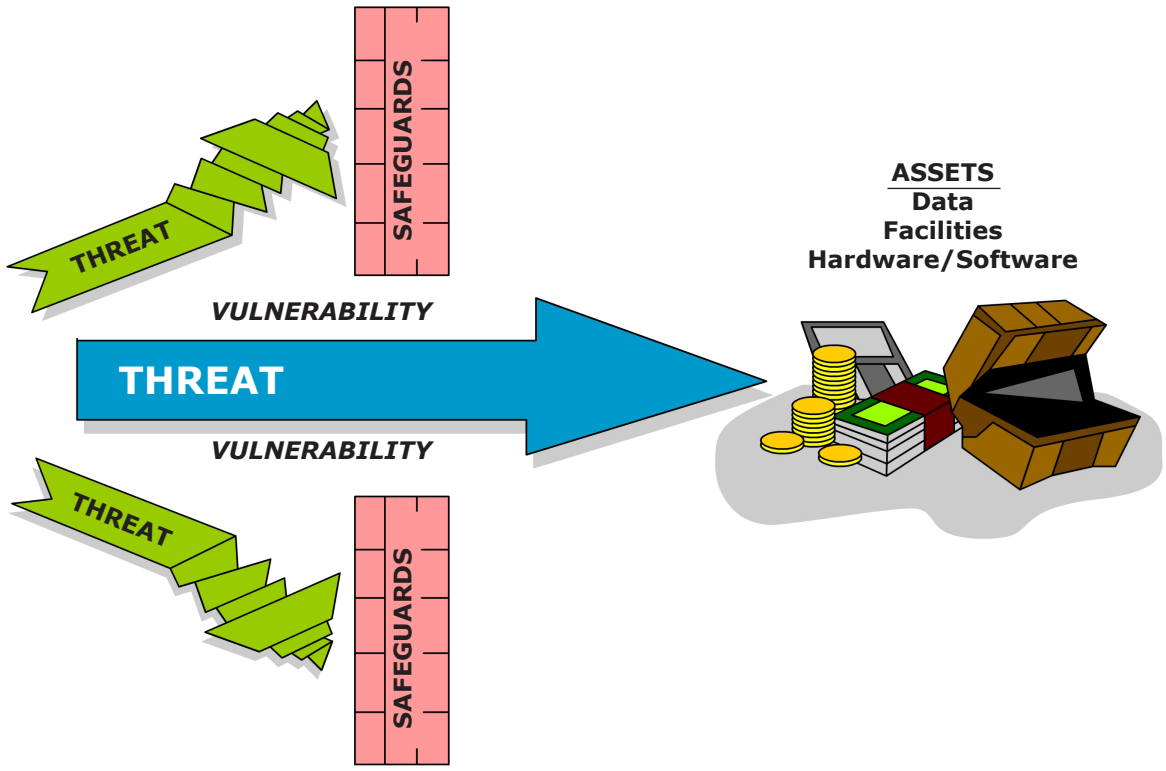


Figure 8.9: Interrelationship vulnerabilities, threats and assets

3. Interpreting Risk Analysis Results

The risk assessment is used to support two related functions which are the acceptance of risk and the selection of cost-effective controls. To accomplish these functions, the risk assessment must produce a meaningful output that reflects what is truly important to the organisation. Limiting the risk interpretation activity to the most significant risks is another way that the risk management process can be focused to reduce the overall effort while still yielding useful results.

If risks are interpreted consistently across an organisation, the results can be used to prioritise systems to be secured.

8.1.4 Risk Analysis

A ***risk analysis*** involves identifying the most probable threats to an organisation and analysing the related vulnerabilities of the organisation to these threats. It is the process of examining a system and its operational context to determine possible exposures and the potential harm they can cause.

Thus, the first step in a risk analysis is to identify and list all exposures in the computing system of interest. Then, for each exposure, identify possible controls and their costs. The last step is a cost-benefit analysis.

8.1.4.1 Steps of Risk Analysis

Risk analysis is performed in many different contexts. Risk analysis for security is adapted from more general management practices, placing special emphasis on the kinds of problems likely to arise from security problems.

Risk analysis approaches normally slightly different between one organisation to another but the basic activities are still the same.

The six basic steps of risk analysis for security risks in computing system (see Figure 8.10).

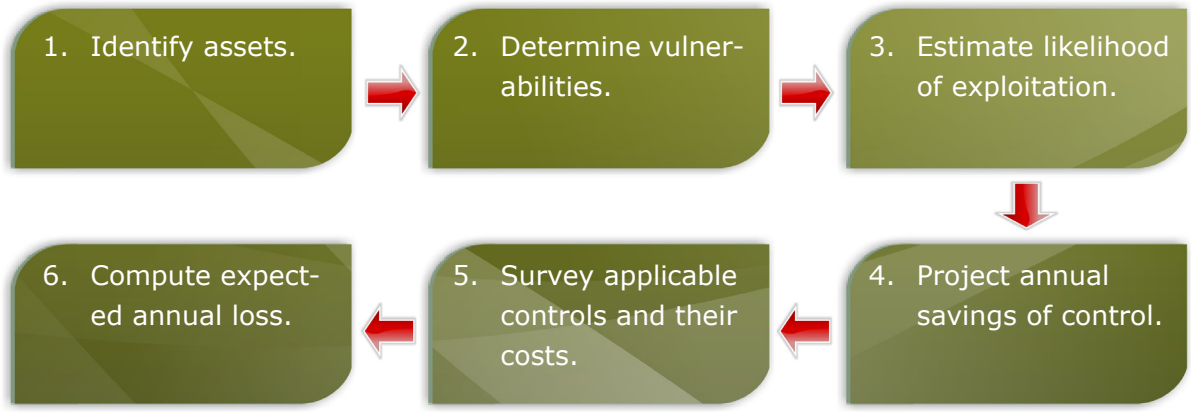


Figure 8.10: The six basic steps of risk analysis for security risks in computing system

1. Identify Assets

The first step of a risk analysis is to identify the assets of computing system. The assets can be considered in categories as described in the following Table 8.4.

Table 8.4: Identifying the Assets of Computing System

The Assets	Details
Hardware	Processors, boards, keyboards, monitors, terminals, microcomputers, workstations, tape drives, printers, disks, disk drives, cables, connections, communications controllers, communication media and any devices that are connected to the computing system.
Software	Source programs, object programs, purchased programs,

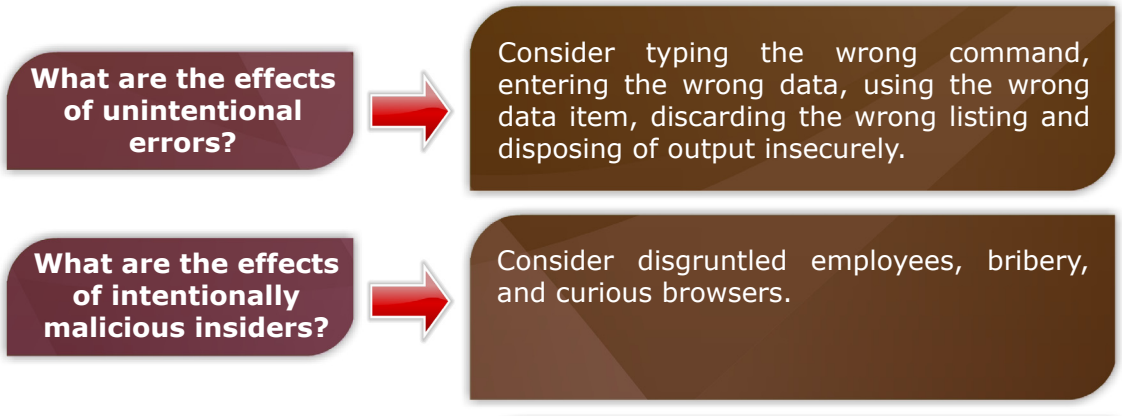
	in-house programs, utility programs, operating systems, system programs such as compiler and maintenance diagnostic programs.
Data	Data used during execution, stored data on various media, printed data, archival data, update logs and audit records.
People	The skills needed to run the computing system or specific program.
Documentation	Programs, hardware, software, systems, administrative procedures and the entire system.
Supplies	Paper, forms, laser cartridges, magnetic media and printer fluid.

It is essential to tailor this list to the organisation situation. Different organisation will have different list of assets to protect and different valuable assets.

2. Determine Vulnerabilities

This step will determine the possible vulnerabilities of the assets from the process of identifying assets. This step requires imagination such as to predict what damage might occur to the assets and from what source. The clear idea of the nature of vulnerabilities can be derived from the need to ensure the three basic goals of computer security that are confidentiality, integrity and availability. Thus, vulnerability is any situation that could cause loss of confidentiality, integrity and availability.

Examples of questions that can be asked to determine the vulnerabilities are (see Figure 8.11).



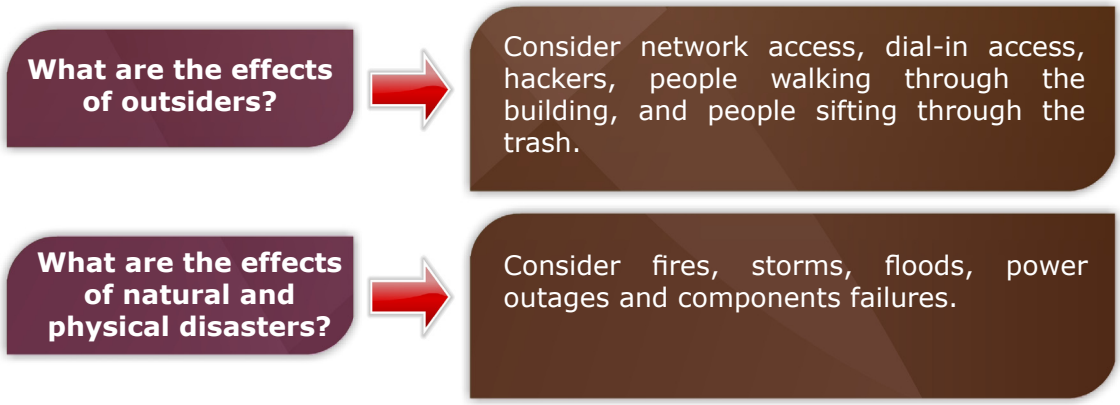


Figure 8.11: Examples of questions that can be asked to determine the vulnerabilities

A matrix as in Table 8.5 and 8.6 can be used to organise the way the organisation considers threats and assets, and to be a guide to stimulate thinking.

Table 8.5: Assets and Security Properties

Asset	Confidentiality	Integrity	Availability
Hardware			
Software			
Data			
People			
Controls			
Documentation			
Supplies			

Table 8.6: Assets and Attacks

Asset	Confidentiality	Integrity	Availability
Hardware		Overloaded, destroyed, tampered with	Failed, stolen, destroyed, unavailable
Software	Stolen, copied, pirated	Impaired by Trojan horse, modified, tampered with	Deleted, misplaced, usage expired
Data	Disclosed, accessed by outsiders, inferred	Damaged (software error, hardware error, user error)	Deleted, misplaced, destroyed

People			Deleted, misplaced, usage expired
Controls			Controls
Documentation			Lost, stolen, destroyed
Supplies			Lost, stolen, damaged

From Table 8.6, it shown that one vulnerability can affect more than one asset or cause more than one type of loss.

3. Estimate Likelihood of Exploitation

This step determines how often each exposure is likely to be exploited. Likelihood of occurrence relates to the stringency of the existing controls and the likelihood that someone or something will evade the existing controls. The techniques that can be used in this step are classical probability, frequency probability and subjective probability.

4. Compute Expected Loss

This step determines the likely loss if the exploitation does indeed occur. In this step, all cost involves must be determine include the hidden cost and all cost that should be spend for the potential vulnerabilities.

5. Survey and Select New Controls

After understand the systems' vulnerabilities and the likelihood of exploitation, the analysis of the controls should be done to see which of the vulnerabilities address the risks. The objective is to match each of the vulnerability with at least one appropriate security technique. Then, use the expected loss estimates to help the organisation to decide which controls are the most cost effective for a given situation. The following questions will be used as the guideline to select the appropriate controls:

- What criteria are used for selecting controls?
- How do controls affect what they control?
- Which controls are best?

6. Project Saving

By this point in the risk analysis activities, the controls that address each vulnerability in the list are identified. The next step is to determine whether the costs outweigh the benefits or preventing or mitigating the risks. The effective cost of a given control is the actual cost of control minus any expected loss from using the control. Thus, the true

cost of a control may be positive if the control is expensive to administer or introduces new risk in another area of the system. Or the cost can even be negative if the reduction in risk is greater than the cost of the control.

8.2 TOOLS AND TECHNIQUES

Many tools can be used to enhance the risk management process. Risk assessments tools help identify relationships, causes and effects. They assist in prioritising decisions and facilitate effective management of the risk management process.

The following tools as listed in Figure 8.12 can be used during the various phases of risk assessment to add objectivity and structure to the process.

Figure 8.12: Risk assessment tools

Let us look into details each of the assessment tools as displayed in Figure 8.12.

Affinity Grouping

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

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

This is to identify the cause and effect in relationships between the risks and the factors. 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 Diagraphs

This is 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, it is facilitating the risk prioritisation.

PERT (Program Evaluation and Review Technique) Charts

PERT Charts is a diagram depicting the interdependencies between project activities and, 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 or 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 risk management plan is a comprehensive plan documenting how risks will be managed on a given project. It contains processes, activities, milestones, organisations, 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.

8.3 CHOOSING APPROPRIATE SAFEGUARDS

A primary function of computer security risk management is the identification of appropriate controls. In designing or reviewing the security of a system, it may be obvious that some controls should be added because they are required by law or because they are clearly cost-effective.

It may also be just as obvious that other controls may be too expensive by considering both monetary and non-monetary factors.

> For example, it may be immediately apparent to a manager that closing and locking the door to a particular room that contains local area network equipment is a needed control, while posting a guard at the door would be too expensive and not user-friendly.

In every assessment of risk, there will be many areas for which it will not be obvious what kinds of controls are appropriate. Even considering only monetary issues, such as whether a control would cost more than the loss it is supposed to prevent, the selection of controls is not simple.

However, in selecting appropriate controls, managers need to consider many factors, including:

- Organisational policy, legislation and regulation;
- Safety, reliability and quality requirements;
- System performance requirements;
- Timeliness, accuracy and completeness requirements;
- The life cycle costs of security measures;
- Technical requirements; and
- Cultural constraints.

One method of selecting safeguards uses a "what if" analysis. With this method, the effect of adding various safeguards and therefore reducing vulnerabilities is tested to see what difference each makes with regard to cost, effectiveness, and other relevant factors, such as those listed above. Trade-offs among the factors can be seen. The analysis of trade-offs also supports the acceptance of residual risk. This method

typically involves multiple iterations of the risk analysis to see how the proposed changesaffect the risk analysis result.

Another method is to categorise types of safeguards and recommend implementing them for various levels of risk. For example, stronger controls would be implemented on high-risk systems than on low-risk systems. This method normally does not require multiple iterations of the risk analysis.

As with other aspects of risk management, screening can be used to concentrate on the highest risk areas. For example once could focus on risks with very severe consequences, such as a very high dollar loss or loss of life or on the threats that are most likely to occur.

SUMMARY

1. Risk management is a key management process that must be used at every level whether managing a project, a program or an enterprise.
2. It also a strategic tool to more effectively manage increasingly sophisticated, diverse and geographically expansive business opportunities.
3. Managing risk a key to keeping business competitive and must be done by managers at all level.
4. Common business risks include management of treasury, revenue, contracts, fraud, environment, regulatory issues, business continuity and technology.
5. Technology is a business risk that is so important and must be specifically managed.
6. Technology risks include security, privacy, information technology operations, business systems and effectiveness, information systems testing, and management of business continuity, reliability and performance, information technology assets, project risks and change. good and bad security practices in a fair and concise manner.

GLOSSARY

Annualised Loss Expectancy (ALE)	How much an event is expected to cost per year.
Qualitative Risk Assessment	The process of subjectively determining the impact of an event that affects a project, program or business. It usually involves the use of expert judgment, experience or group consensus to complete the assessment.
Quantitative Risk Assessment	The process of objectively determining the impact of an event that affects a project, program or business. It usually involves the use of metrics and models to complete the assessment.
Risk	The possibility of suffering harm or loss.
Risk Management	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 threats.
Single Loss Expectancy (SLE)	The monetary loss or impact of each occurrence of a threat.

CHALLENGE QUESTIONS

1. Which of the following best defines risk?

   A. The risks still remaining after an iteration of risk management.
   B. The loss that results when 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.

2. Which of the following is a technology risk?

   A. Business continuity management.
   B. Fraud.
   C. Contract management.
   D. Treasury management.

3. Briefly define what Gantt chart is.

4. Determine the basic activities of risk assessment.

CHALLENGE EXERCISE

Given a scenario below, learner is required to clarify the solution for the questions.

You are explaining your risk management plan to a new team member just brought on as part of a college internship program. What would your answer or your response if the intern asks you the following questions?

1. With respect to impact, what does a threat do to a risk?
2. What is the difference (compare and contrast) between accepting risk, transferring risk and mitigating risk?

REFERENCES

Charles P. Pleeger (2003). *Security in Computing*. New Jersey, United States: Prentice Hall.

Michael G. Solomon & Mike Chapple (2005). *Information Security Illuminated*. Sudbury, Massachusetts: Jones and Bartlett Publishers.

NIST. *An Introduction to Computer Security: The NIST Handbook*. SP 800-12.

Wm. Arthur Conklin et.al. (2005). *Principles of Computer Security*. Singapore: McGraw-Hill Education (Asia).