


What is Risk?



- Risk refers to the degree of **uncertainty** or expectation that an adverse event may cause damage to the system
- Risks are categorized into different levels according to their estimated impact on the system
- A risk matrix is used to scale risk by considering the **probability, likelihood, and consequence or impact** of the risk

Risk Levels

Risk Level	Action
Extreme or High	<ul style="list-style-type: none"> ➤ Immediate measures should be taken to combat risk ➤ Identify and impose controls to reduce risk to a reasonably low level
Medium	<ul style="list-style-type: none"> ➤ No urgent action is required ➤ Implement controls as soon as possible to reduce risk to a reasonably low level
Low	<ul style="list-style-type: none"> ➤ Take preventive steps to mitigate the effects of risk

Risk Matrix

Probability		Consequences					
		Insignificant	Minor	Moderate	Major	Severe	
81 - 100%	Likelihood	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%	High Probability	Low	Medium	High	High	Extreme	
41 - 60%	Equal Probability	Low	Medium	Medium	High	High	
21 - 40%	Low Probability	Low	Low	Medium	Medium	High	
1 - 20%	Very Low Probability	Low	Low	Medium	Medium	High	

Note: This is an example of a risk matrix. Organizations need to create their own risk matrix based on their business needs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Risk?

Risk refers to the degree of uncertainty or expectation of potential damage that an adverse event may cause to the system or its resources, under specified conditions. Alternatively, risk can also be:

- The probability of the occurrence of a threat or an event that will damage, cause loss to, or have other negative impacts on the organization, either from internal or external liabilities.
- The possibility of a threat acting upon an internal or external vulnerability and causing harm to a resource.
- The product of the likelihood that an event will occur and the impact that the event might have on an information technology asset.

The relation between Risk, Threats, Vulnerabilities, and Impact is as follows:

$$\text{RISK} = \text{Threats} \times \text{Vulnerabilities} \times \text{Impact}$$

The impact of an event on an information asset is the product of vulnerability in the asset and the asset's value to its stakeholders. IT risk can be expanded to

$$\text{RISK} = \text{Threat} \times \text{Vulnerability} \times \text{Asset Value}$$

In fact, the risk is the combination of the following two factors:

- The probability of the occurrence of an adverse event
- The consequence of the adverse event

Risk Level

Risk level is an assessment of the resulted impact on the network. Various methods exist to differentiate the risk levels depending on the risk frequency and severity. One of the common methods used to classify risks is to develop a two-dimensional matrix.

Working out the frequency or probability of an incident happening (likelihood) and its possible consequences is necessary to analyze risks. This is referred to as the level of risk. Risk can be represented and calculated using the following formula:

$$\text{Level of Risk} = \text{Consequence} \times \text{Likelihood}$$

Risks are categorized into different levels according to their estimated impact on the system. Primarily, there are four risk levels, which include extreme, high, medium, and low levels. Remember that control measures may decrease the level of a risk, but do not always entirely eliminate the risk.

Risk Level	Consequence	Action
Extreme or High	Serious or Imminent danger	<ul style="list-style-type: none">➤ Immediate measures are required to combat the risk➤ Identify and impose controls to reduce the risk to a reasonably low level
Medium	Moderate danger	<ul style="list-style-type: none">➤ Immediate action is not required, but action should be implement quickly➤ Implement controls as soon as possible to reduce the risk to a reasonably low level
Low	Negligible danger	<ul style="list-style-type: none">➤ Take preventive steps to mitigate the effects of risk

Table 1.1: Risk Levels

Risk Matrix

The risk matrix scales the risk occurrence or likelihood probability, along with its consequences or impact. It is the graphical representation of risk severity and the extent to which the controls can or will mitigate it. The Risk matrix is one of the simplest processes to use for increased visibility of risk; it contributes to the management's decision-making capability. The risk matrix defines various levels of risk and categorizes them as the product of negative probability and negative severity. Although there are many standard risk matrices, individual organizations must create their own.

Probability	Consequences					
		Insignificant	Minor	Moderate	Major	Severe
81 - 100%	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%	High Probability	Low	Medium	High	High	Extreme
41 - 60%	Equal Probability	Low	Medium	Medium	High	High
21 - 40%	Low Probability	Low	Low	Medium	Medium	High
1 - 20%	Very Low Probability	Low	Low	Medium	Medium	High

Table 1.2: Risk Matrix

The above table is the graphical representation of a risk matrix, which is used to visualize and compare risks. It differentiates the two levels of risk and is a simple way of analyzing them.

- Likelihood: The chance of the risk occurring
- Consequence: The severity of a risk event that occurs

Note: This is an example of a risk matrix. Organizations must create individual risk matrices based on their business needs.

Risk Management



■ Risk management is the process of **reducing and maintaining risk at an acceptable level** by means of a well-defined and actively employed security program

Risk Management Phases

Risk Identification	■ Identifies the sources , causes, consequences, and other details of the internal and external risks affecting the security of the organization
Risk Assessment	■ Assesses the organization's risk and provides an estimate of the likelihood and impact of the risk
Risk Treatment	■ Selects and implements appropriate controls for the identified risks
Risk Tracking	■ Ensures appropriate controls are implemented to handle known risks and calculates the chances of a new risk occurring
Risk Review	■ Evaluates the performance of the implemented risk management strategies

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Risk Management

Risk management is the process of identifying, assessing, responding to, and implementing the activities that control how the organization manages the potential effects of risk. It has a prominent place throughout the security life cycle and is a continuous and ever-increasing complex process. The types of risks vary from organization to organization, but the act of preparing a risk management plan is common to all organizations.

Risk Management Objectives

- Identify potential risks—this is the main objective of risk management
- Identify the impact of risks and help the organization develop better risk management strategies and plans
- Prioritize the risks, depending on the impact or severity of the risk, and use established risk management methods, tools, and techniques to assist in this task
- Understand and analyze the risks and report identified risk events.
- Control the risk and mitigate its effect.
- Create awareness among the security staff and develop strategies and plans for lasting risk management strategies.

Risk management is a continuous process performed by achieving goals at every phase. It helps reduce and maintain risk at an acceptable level utilizing a well-defined and actively employed security program. This process is applied in all stages of the organization, for example, to specific network locations in both strategic and operational contexts.

The four key steps commonly termed as risk management phases are:

- Risk Identification
- Risk Assessment
- Risk Treatment
- Risk Tracking and Review

Every organization should follow the above steps while performing the risk management process.

- **Risk Identification**

The initial step of the risk management plan. Its main aim is to identify the risks—including the sources, causes, and consequences of the internal and external risks affecting the security of the organization before they cause harm. The risk identification process depends on the skill set of the people, and it differs from one organization to another.

- **Risk Assessment**

This phase assesses the organization's risks and estimates the likelihood and impact of those risks. Risk assessment is an ongoing iterative process that assigns priorities for risk mitigation and implementation plans, which in turn help to determine the quantitative and qualitative value of risk. Every organization should adopt a risk evaluation process in order to detect, prioritize, and remove risks.

The risk assessment determines the kind of risks present, their likelihood and severity, and the priorities and plans for risk control. Organizations perform a risk assessment when they identify a hazard but are not able to control it immediately. A risk assessment is followed by a regular update of all information facilities.

- **Risk Treatment**

Risk treatment is the process of selecting and implementing appropriate controls on the identified risks in order to modify them. The risk treatment method addresses and treats the risks according to their severity level. Decisions made in this phase are based on the results of a risk assessment. The purpose of this step is to identify treatments for the risks that fall outside the department's risk tolerance and provide an understanding of the level of risk with controls and treatments. It identifies the priority order in which individual risks should be treated, monitored, and reviewed. The following information is needed before treating the risk:

- The appropriate method of treatment
- The people responsible for the treatment
- The costs involved
- The benefits of treatment
- The likelihood of success
- Ways to measure and assess the treatment

- **Risk Tracking and Review**

An effective risk management plan requires a tracking and review structure to ensure effective identification and assessment of the risks as well as the use of appropriate controls and responses. The tracking and review process should determine the measures and procedures adopted and ensure that the information gathered to perform the assessment was appropriate. The review phase evaluates the performance of the implemented risk management strategies. Performing regular inspections of policies and standards, as well as regularly reviewing them, helps to identify the opportunities for improvement. Further, the monitoring process ensures that there are appropriate controls in place for the organization's activities and that all procedures are understood and followed.