



**Certified Network Defender v3**

**MODULE 18**

**RISK ANTICIPATION WITH  
RISK MANAGEMENT**

---

EC-Council Official Curricula



This page is intentionally left blank.



## LEARNING OBJECTIVES

The learning objectives of this module are :

- LO#01: Understand risk management concepts
- LO#02: Learn to manage risk through a risk management program
- LO#03: Learn different risk management frameworks (RMFs)
- LO#04: Learn to manage vulnerabilities through a vulnerability management program
- LO#05: Learn vulnerability assessment and scanning

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

### Learning Objectives

This module introduces you with risk management concepts. The module presents a brief discussion on how proper and systematic risk management helps organizations anticipate and manage risks to an acceptable level. This module covers various phases involved in the implementation and execution of an organization's risk management program. The learning objectives of this module are:

- Understand risk management concepts
- Learn to manage risk through a risk management program
- Learn different risk management frameworks (RMFs)
- Learn to manage vulnerabilities through a vulnerability management program
- Learn vulnerability assessment and scanning
- Discuss Privacy Impact Assessment (PIA)





“ Risk and vulnerability management is a pro-active approach to manage network security ”

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





## LO#01: Understand risk management concepts


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

### **LO#01: Understand Risk Management Concepts**

This section will introduce risk management concepts, key risk indicators (KRIs), key roles, and responsibilities in risk management.



## 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
- It involves identifying, assessing, and responding to the risks by implementing controls to help the organization manage the potential effects
- Risk management has a **prominent** place throughout the system security life-cycle

### Risk Management Benefits:

- Focuses on potential risk impact areas
- Addresses risks according to the risk level
- Improves the risk handling process
- Allows the security officers to act effectively in adverse situations
- Enables effective use of risk handling resources
- Minimizes the effect of risk on the organization's revenue
- Identifies suitable controls for security

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

## Risk Management

Risk management is the process of identifying, assessing, and responding to the risks by implementing activities that control how an organization manages potential risks. Risk management has a prominent place throughout the security life cycle. It is a continuous and increasingly complex process that requires anticipating risks and creating a plan to overcome the risk when it occurs. The type of risks varies by organization, but all organizations should prepare a management plan. Risk management helps save time, money, and efforts.

### Risk Management Objectives

- Identify the potential risks
- Identify the impact of risks and help an organization develop better risk management strategies and plans
- Depending on the impact/severity of the risk, prioritize the risks and use established risk management methods, tools, and techniques to assist
- Understand and analyze the risks and report identified risk events
- Control the risk and mitigate the risk impact
- Create awareness among the security staff; develop long-term, reliable strategies and plans for risk management

### Risk Management Benefits

Risk management provides a structured approach to identifying risks. Having a clear idea of all risks allows an organization to analyze, prioritize, and take the appropriate actions to reduce losses.



## Other Benefits

- Focuses on the potential risk impact areas
- Addresses risks according to a level
- Improves the risk handling process
- Allows security officers to act effectively in adverse situations
- Enables effective use of resources
- Minimizes the impact of risk on an organization's revenue
- Identifies suitable controls for security



## Key Roles and Responsibilities in Risk Management



■ <b>Senior Management:</b> The <b>support</b> and <b>involvement</b> of senior management is required for effective risk management
■ <b>Chief Information Officer (CIO):</b> Responsible for IT planning, budgeting, and performance based on a risk management program
■ <b>System and Information Owners:</b> Responsible for the appropriate security control use to maintain confidentiality, integrity, and availability for an information system
■ <b>Business and Functional Managers:</b> Responsible for making <b>trade-off</b> decisions in the risk management process
■ <b>IT Security Program Managers and Computer Security Officers (ISSO):</b> Responsible for an organization's information security programs
■ <b>IT Security Practitioners:</b> Responsible for implementing <b>security controls</b>
■ <b>Security Awareness Trainers:</b> Responsible for <b>developing</b> and <b>providing</b> appropriate training <b>in</b> the risk management process

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

## Key Roles and Responsibilities in Risk Management

### Senior Management

It is the responsibility of the senior management to supervise the risk management plans of an organization. They develop policies and techniques required to handle common risks. Senior managers, through their expertise, can design the steps required for handling future risks.

### Chief Information Officer (CIO)

The CIO is responsible for executing the policies and plans required for supporting the information technology and computer systems of an organization. The CIO plays a vital role in the formation of basic plans and policies for risk management. The main responsibility of a CIO is to train employees and other executive management regarding the possible risks in IT and its impact on business.

### System and Information Owners

- System and information owners mainly monitor the plans and policies developed for information systems. Their responsibilities include the following:
- Take part in all discussions on the configuration management process
- Keep a record of the information system's components
- Investigate all changes in the information systems and their impact
- Prepare a security status report for all information systems
- Update the security controls required for protecting the information systems
- Update the security related documents on a regular basis



- Examine and evaluate the existing security controls in order to confirm their efficiency in protecting a system

### **Business and Functional Managers**

They are responsible for maintaining all management processes in an organization. They are empowered with the authority to manage almost all processes in an organization. The roles defining functional managers are:

- Development team manager
- Sales manager
- Accounts receivable manager
- Customer service manager

### **IT Security Program Managers and Computer Security Officers (ISSOs)**

ISSOs provide the required support to information system owners with a selection of security controls needed for protecting a system. They also play an important role in the selection and amendment of security controls in an organization.

### **IT Security Practitioners**

IT security practitioners protect the personnel as well as physical and information security in an organization. Their main responsibilities include:

- Framing better security methods in an organization
- Developing methods that fulfill the company's standards
- Examining the company's security approach to risk management and business planning
- Handling and recording security incidents
- Assigning roles and responsibilities for security in an organization
- Supervising the overall security measures taken in an organization

### **Security Awareness Trainers**

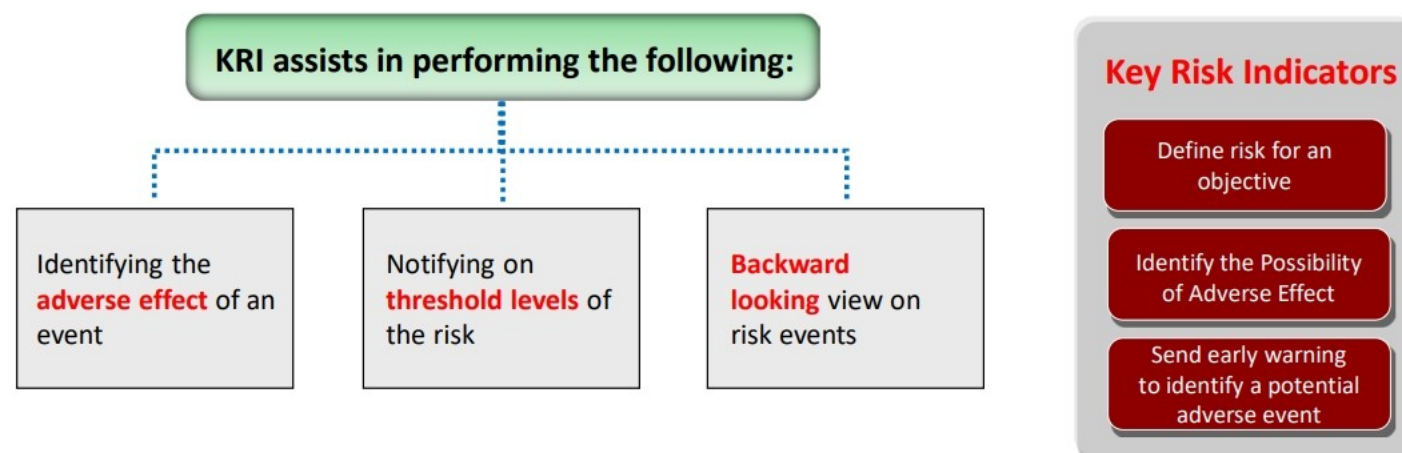
Security awareness trainers provide IT security awareness and training programs in an organization. They are often subject matter experts and ensure that only proper content is included in the program.



## Key Risk Indicators (KRI)



- A key risk indicator (KRI) is an important component of an effective **risk management process** that shows the riskiness of an activity
- **Understanding** the organizational goals is required to identify KRI
- A KRI is a metric showing the risk appetite probability for an organization



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

### Key Risk Indicators (KRI)

KRIs are essential components of an effective risk management process, and indicate the riskiness of an activity at an early stage. An understanding of organizational goals is required to properly identify KRIs. It is a metric that can indicate the risk appetite probability of an organization. KRIs are the most important indicators of an organization's overall health, helping reduce loss and prevent risk exposure. Risk exposure is prevented by measuring the risk profiles and risk situations in advance before the risk event occurs.

#### Role of KRIs

- Identify current risk exposure and emerging risk trends in order to provide an early warning and proactive action
- Event impact identification
- Threshold level notifications
- Backward looking view on risk events, enabling learning lessons from the past events
- Highlight weaknesses of the existing controls and allow strengthening of poor controls
- Facilitate the risk-reporting and escalation process
- Provide an indication that the risk appetite and tolerance are reached
- Provide real-time actionable intelligence to decision-makers and risk managers

#### Features of Effective KRIs

- **Quantifiable Metrics:** Should be measurable (number, count, or percentage)
- **Predictable:** Should provide early warning signals



- **Comparable:** Should be able to track over a period of time
- **Informational:** Should measure the status of the risk and control

KRIs should accurately measure and reflect any negative impact on an organization's key performance indicators (KPI). KPI is a metric that assesses the progress of an organization toward its goals, and provides leading indicator information about emerging risks from external events that impact the demand for an organization's products or services. KRIs represent key ratios that an organization tracks as indicators of evolving risks and potential opportunities, and guide an organization's responses. KRIs should be reported regularly; proper escalation methods and plans enable timely reporting to the management. KRIs have different escalation levels.

Management identifies the KRIs to execute its strategic initiatives by mapping risks. An effective method for developing KRIs is to first identify risk events that could impact an organization's financial status, and then find the intermediate and root cause for the risk event. The indicator assists management with responding to the risk event in advance.





## LO#02: Learn to manage risk through risk management program

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

### **LO#02: Learn to Manage Risk through Risk Management Program**

This section explains risk management phases involved in an organization's risk management program.



## Risk Management Phase: Risk Identification

Risk identification is the foundation and first step of risk management. It lists risks and their characteristics before such risks harm an organization. This process depends on the skill set of individuals and also differs by organization. It identifies the sources, causes, and consequences of all internal and external risks that impact organizational security. The identified risks are recorded in a risk register and further analyzed. Thus, risk identification is an iterative process. The purpose of risk identification is to generate a list of threats and opportunities based on risk events that respectively prevent and enhance the achievement of objectives.

### Role of Risk Identification

- **Environment:** Risks associated with the environment such as crowded workspaces, clutter, hot/cold environments, smoking, poor lighting, and electrical hazards
- **Equipment:** Risks associated with equipment such as poor condition, non-functioning devices, unavailability, and task-inappropriate equipment
- **Client:** Risks associated with clients because of conditions changing, unpredictable movements, and poor communication
- **Tasks:** Tasks-related risks include insufficient time allocated, repetitive tasks, work design, task organization, maintaining a fixed posture, poor postures, and insufficient employee numbers

### Risk Identification Steps

- **Establishing Context:** The employee defines the external and internal environment and understands the current conditions in which an organization operates



- **Quantifying Risks:** Determines the impact of risk and calibrates the possible outcome of the risks

### Main Elements in Risk Identification

- **Description/Event:** An occurrence or a particular set of circumstances
- **Causes:** Factors that may contribute to a risk occurring
- **Consequences:** Impact of an event

### Priorities of Risk Identification

Know what to consider when identifying risks. This ensures the major issues are not missed.

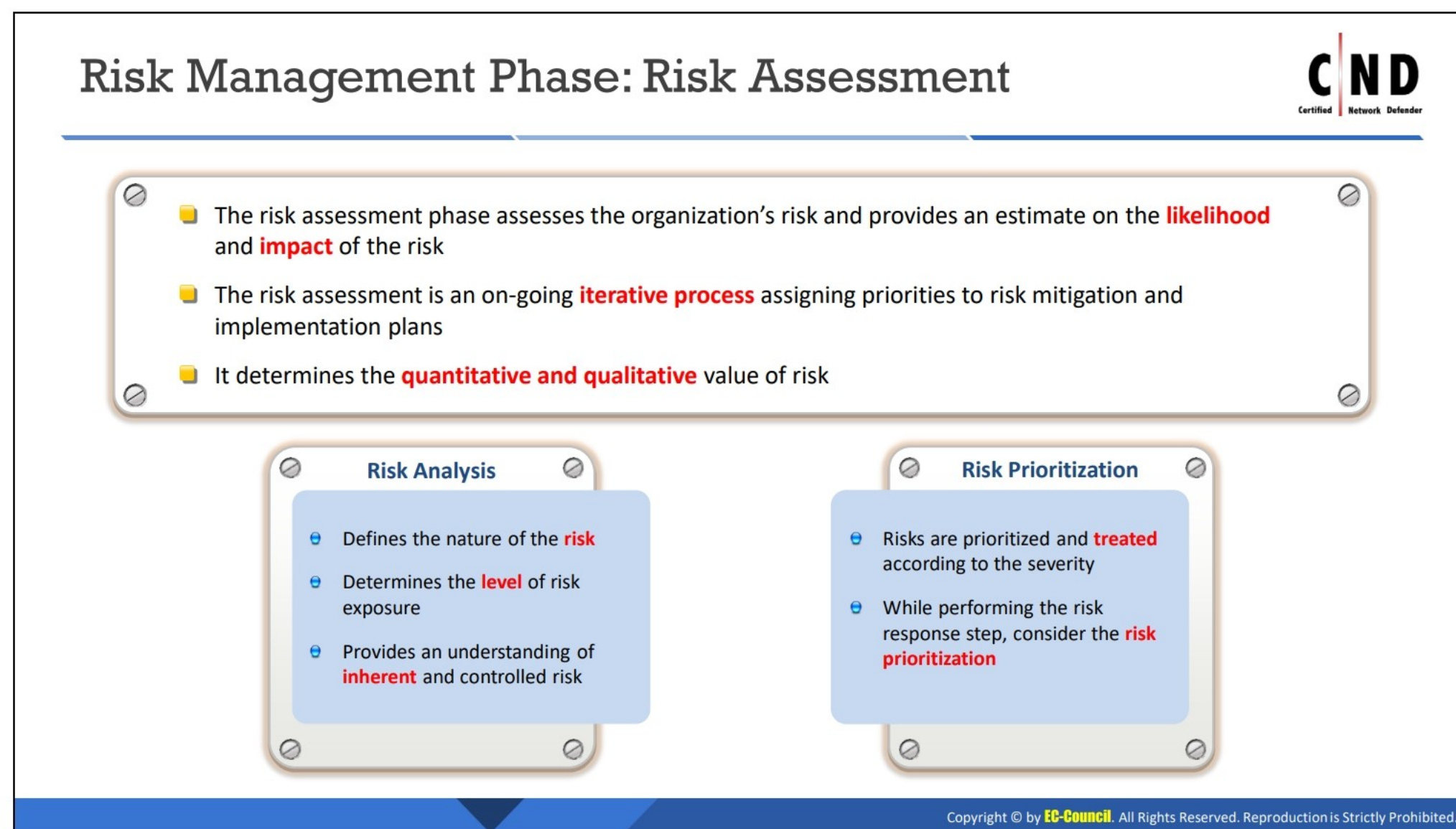
Gather the information taken from multiple sources. The network defender needs to discuss the old, current, and evolving issues; data analysis; review of performance indicators; data loss; and scenario planning with an organization's stakeholders to determine critical risk information.

Use risk identification tools and techniques for acquiring relevant and up-to-date information of risks an organization faces. The techniques used for risk identification include checklists, flow charts, and systems analysis.

Document the risks, which includes:

- Risk description
- How and why the risk occurs
- Existing internal controls that may mitigate the likelihood or consequences of the risks
- Methods that identify the risks
- Scope covered by the identification
- Participants in the risk identification
- The information sources consulted
- Analyze the risk identification process's effectiveness.





## Risk Management Phase: Risk Assessment

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

Risk assessment determines the types of risks that exist, likelihood and severity of risks, and priorities and plans for risk control. An organization performs risk assessment when it identifies a hazard but cannot control it immediately. After risk assessment, all information facilities should be updated at regular intervals.

After assessing risks, they are prioritized based on their severity or impact. The prioritized list is crucial to developing an effective plan that can handle the task sequence list; it also helps allocate resources thereof. The numbers below indicate risk priority based on severity:

- **1–2:** These risks need to be eliminated immediately (usually within 24 hours); if elimination is not possible, then the risk of the hazard needs to be reduced to a lower rating by implementing at least one control measure.
- **3–4:** These risks need to be eliminated or the hazard needs to be controlled within a reasonable timeframe.
- **5–6:** Eliminate this type of risk as soon as possible or control the hazard when possible.



## Steps in Risk Assessment

- **Risk Analysis:** This step involves analyzing the risk of vulnerabilities and threats in order to provide an understanding of the inherent and controlled risks. Risk analysis defines the nature of the risk and determines the level of risk exposure.
- **Risk Prioritization:** In order to identify the various risks with the same severity, the risks should be prioritized and rated. This way, an appropriate response plan may be designed. The prioritization depends on the goals and resources of an organization. Consider the following for risk prioritization:
  - Immediate and future impact of a risk on an organization's goals, assets, other organizations, and the nation in order to prioritize risks
  - Expected loss because of a risk
  - Relationship of a risk and/or mitigation to other risks and/or mitigations
  - Managing the impact of threats from a risk



## Risk Levels



- Risks are categorized into different levels according to their estimated impact on the system
- The **impact level** of a risk depends on the value of assets and resources it affects, and the severity of the damage

Risk Level	Action
Extreme / High	<ul style="list-style-type: none"> <li>Immediate measures should be performed to combat risk</li> <li>Identify and <b>impose controls</b> to reduce risk to a reasonably low level</li> </ul>
Medium	<ul style="list-style-type: none"> <li>Immediate action is not required, but it should be <b>implemented</b> quickly</li> <li>Implement controls as soon as possible to reduce risk to a reasonably low level</li> </ul>
Low	<ul style="list-style-type: none"> <li>Take <b>preventive steps</b> to mitigate the effects of risk</li> </ul>

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

## Risk Levels


Risks are categorized into different levels—“high,” “medium,” and “low,” according to their estimated impact on a system. The impact level of a risk depends on the value of the assets and resources that the risk impacts, and the severity of the damage. The risk levels also present the actions that an organization’s staff should take for each risk level.

Risk Level	Action
Extreme/High	<p>Immediate measures should be taken to isolate, eliminate, and substitute the risk through effective risk controls</p> <p>Identify and impose controls and define strict timelines to reduce risk to a reasonably lower level, though the existing system can continue to operate</p> <p>Stop the activity unless the risk is reduced to a low or medium level</p>
Medium	<p>Immediate action is not required, but measures should be implemented quickly</p> <p>Implement controls as soon as possible to reduce risk to a reasonably lower level</p>
Low	<p>Take preventive steps to mitigate the impact of a risk</p> <p>Ignore them as they generally do not pose any significant problem, but periodical review is necessary to ensure the controls remain effective</p>

Table 18.1: Risk Level and Action



## Risk Matrix



■ A risk matrix is used to scale risk by considering the **probability, likelihood**, and **consequence/impact** of the risk

Probability		Consequences				
		Insignificant	Minor	Moderate	Major	Severe
81–100%	Likelihood	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

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

## Risk Matrix

The risk assessment matrix is a useful tool to identify the probability of failure and high-risk areas. In addition to risk levels, a risk-level matrix needs to be developed to measure or assess a risk. Here,

$$\text{Risk rating} = \text{Probability(Likelihood)} \times \text{Severity},$$

Where,

Probability (Likelihood) measures the likelihood that an uncertain event will occur; and severity is the degree of the impact of damage caused by an uncertain event. It is classified as severe, major, moderate, minor, or insignificant.

The priority of an event is classified into five categories and mapped against the severity and probability of the risk.

### Features of a Risk Matrix

- Quantitative/semi-quantitative hazard analysis tool
- Simple and easy to understand
- Clearly defined tolerable and non-tolerable ranges before developing a risk matrix
- Detailed descriptions of all consequences within the range
- Using the orders of magnitudes and constant likelihood range to cover the total risks
- Providing good guidance for effective hazard analysis in a qualitative manner, which may not need prior knowledge for qualitative analysis
- Flexible enough to adapt for different risk targets that are specific for an organization
- No prior software knowledge is required, as it can be executed using a software



## Risk Management Phase: Risk Treatment



■ Risk treatment is a process of selecting and implementing **appropriate controls** on the identified risks

■ Risks are addressed and treated based on its **severity level**

■ Decisions made in this phase are based on the results of a **risk assessment**

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

### Risk Management Phase: 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 the risks' severity level. Some of these measures are discussed below.

Decisions made in this phase are based on the results of a risk assessment. This step identifies treatments for risks that fall outside the department's risk tolerance and provide an understanding of the level of risk along with controls and treatments. It identifies the priority order in which individual risks should be treated, monitored, and reviewed. Before treating the risk, the network defender needs to gather the information about the

- Appropriate method of treatment;
- Users responsible for treatment;
- Costs involved;
- Benefits of treatment;
- Likelihood of success; and
- Ways to measure and assess the treatment.

Once the network defender has decided how to treat the identified risks, develop and regularly review the risk management plan. The different options for risk treatment include avoiding the risk itself (avoiding the activities that lead to increased risk probability), reducing the risk (reducing the likelihood of the risk occurring and reducing the impact if the risk occurs), transferring the risk (shifting the risk responsibilities to another party through insurance or partnership), and accepting the risk (if it cannot be avoided or transferred).



### **Actions to Minimize or Eliminate Risk**

- Develop a risk control plan
- Find the impact of risk control on a service delivery
- Constraints required for risk control are identified and considered when completing the risk control plan
- Implementation of risk control strategies
- Uncontrollable risks
- Client resistance to risk control
- Communicate with support workers/other workers during risk control
- Completely document the risk control plan as a part of the risk control process



Risk Treatment Process	
Eliminate the Risk	Eliminating the risk by applying <b>controls</b> to reduce the threat of exploiting the vulnerability to <b>zero</b>
Transfer the Risk	<b>Transferring</b> the risk treatment responsibility to <b>another party</b> or organization
Mitigate the Risk	<b>Reducing</b> the risk associated with a threat or <b>vulnerability</b> by implementing direct or competing controls
Accept the Risk	Risks are accepted when the <b>effort</b> to address, transfer, or mitigate has exceeded the impact of the risk on the network
Risk Avoidance	<b>Eliminating</b> the cause and consequences of the risk

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

## Risk Treatment Process

A risk treatment process can change the likelihood of risk occurrence owing to the risk treatment options available. These options help us understand what risk treatment constitutes and help mitigate or manage the risks.

### Types of Risk Treatment Process Options

- **Eliminate the Risk:** Eliminating the risk by applying controls to reduce the threat of exploiting the vulnerability to zero
- **Transfer the Risk:** Transferring the risk factor to a third party that can manage the risk levels
- **Mitigate the Risk:** Reducing the risks associated with a threat or vulnerability by implementing direct or competing controls
- **Accept the Risk:** The risk factor should be at an acceptable level; risks are accepted when the efforts to address, transfer, or mitigate them exceed their impact on a network
- **Risk Avoidance:** Avoiding the factor that enhances the risk factor of any process in the business or finding an alternative that goes well with business needs—such as not allowing the use of laptops in an organization to avoid associated risks
- **Reduce the Risk:** Finding ways to reduce the likelihood rate of risk to an acceptable level—such as by implementing safety controls

The steps taken in risk treatment differ by each case. Stakeholders and process owners mutually decide these steps. The key points while considering risk treatments are as follows:

- Implement an appropriate risk treatment option



- Ensure adequate resources are available while implementing the risk treatment plan
- The risk treatment plan should reduce the risk factor to a certain acceptable level
- Remedial actions should be taken for risks that need to be handled immediately
- Note: The risk treatment options do not always mitigate risks completely. Often, residual risks persist, and these need to be considered as well.



## Risk Treatment Plan



- It is the action plan describing how you plan to **respond** to potential risks
- A risk treatment plan document must be produced as part of a **certified ISO 27001** information security management system

### Risk Treatment Plan

- Proposed security controls with priorities and deadlines
- Required resources
- Roles and responsibilities of stakeholders responsible for the proposed action
- Performance
- Reporting and monitoring requirements

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

## Risk Treatment Plan

The risk treatment plan is the action plan that describes the plan to respond to potential risks. It provides a summary of the identified risks, every risk's designed response, parties responsible for all risks, and target date for risk treatment. It is one of the essential documents an organization should produce as part of a certified ISO 27001 information security management system.

### Steps for Risk Treatment Plan

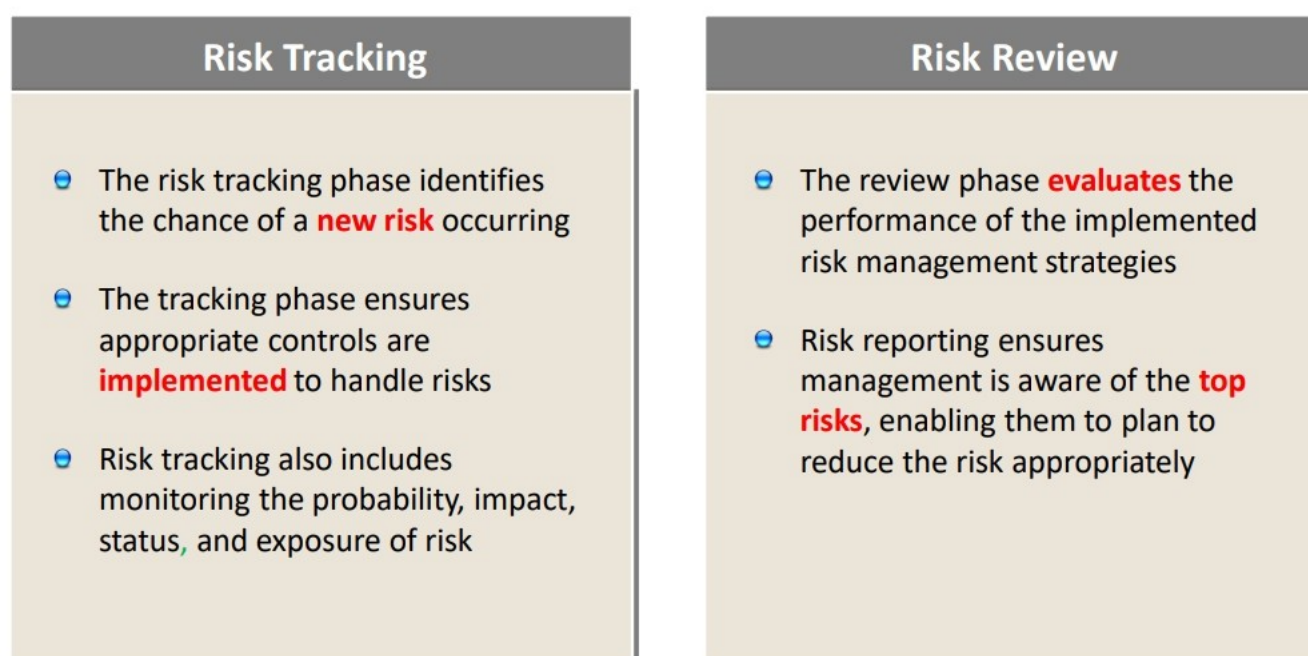
Developing a risk treatment plan requires determining the level of treatment plan at each risk level. For example, what treatment level would be necessary for moderate, minor, or high risks, respectively? Or what improvement opportunities are available to offset risks?

To ensure risk treatment plans are implemented corrected and monitored accurately, the network defender needs to ensure

- Whether the right structure is used to support the treatment plan;
- Availability of adequate resources for those involved in mitigating risks;
- Communication within the treatment plan and with key stakeholders;
- That the right risk treatment plan is implemented through accurate and timely risk analysis;
- The owner of the treatment plan can specify how the implementation will be monitored, including increasing or decreasing risk levels; and
- The treatment plan is routinely reviewed for effectiveness and risk levels.



## Risk Management Phase: Risk Tracking & Review



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

### Risk Management Phase: Risk Tracking & Review

For the risk management process, well-planned and regular monitoring and review are required to identify new risks and reduce them appropriately.

#### Risk Tracking

Risk tracking identifies the chance of a new risk; it includes monitoring the probability, impact, status, and exposure of risks. In this step, the identified risks are regularly reviewed and the changes in the actions or events are documented—for example, the risk evaluation is modified when security controls that reduce risk and record new identified risks are implemented.

#### Risk Review

Reviewing the effectiveness of the implemented risk management strategies regularly helps understand the shortcomings of the security controls and enhance the implemented security controls. It enables an organization to maintain its risk management objectives as well as keep its context up-to-date and accurate.





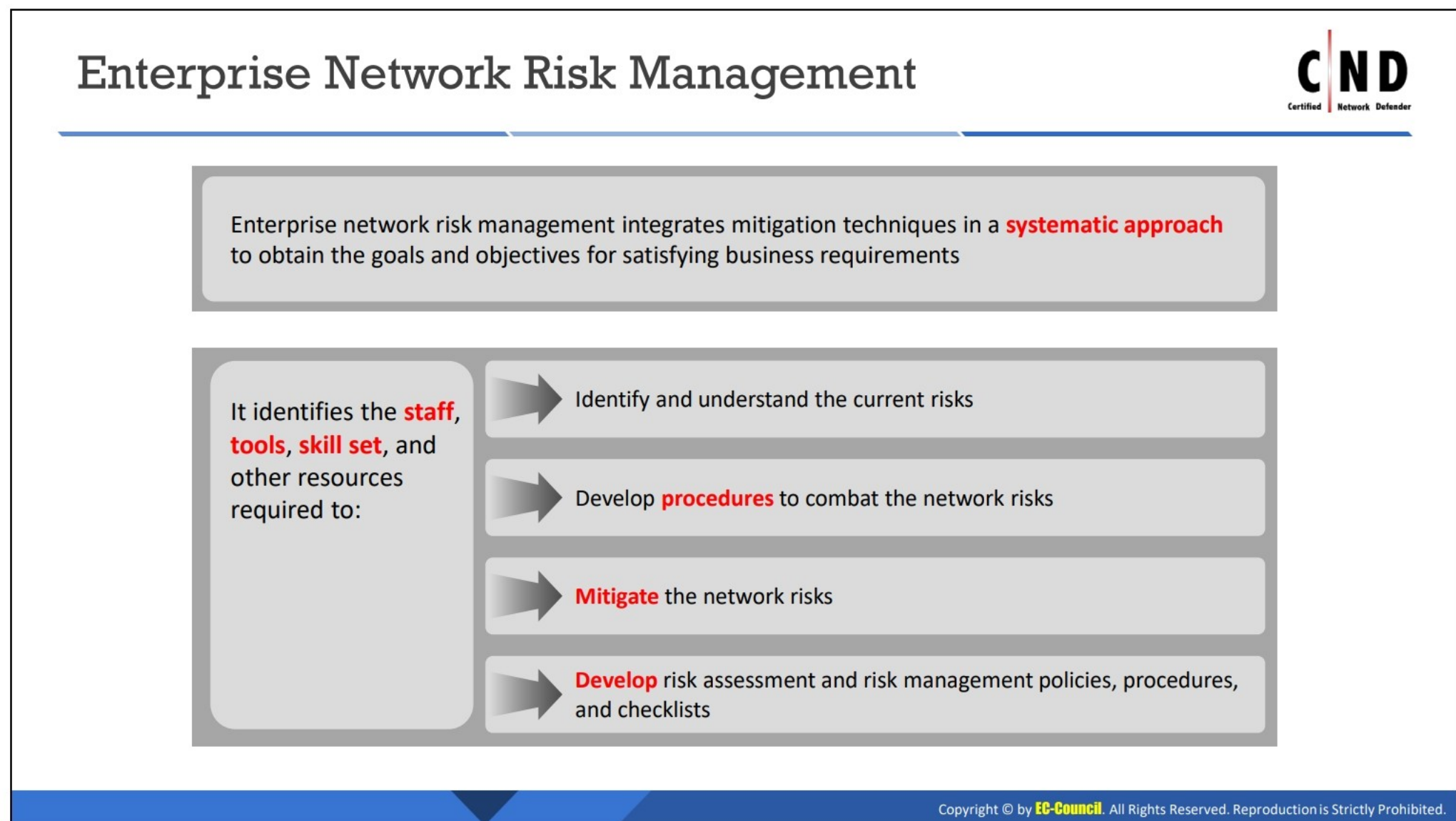
### LO#03: Learn different risk management frameworks

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

## LO#03: Learn Different Risk Management Frameworks

Organizations establish an RMF to understand the overall risk level. Every organization has different infrastructure and potential risks specific to their infrastructure. An organization's strategic objectives and stakeholders needs determine the RMF required. Understanding various frameworks will enable an organization to choose the most appropriate framework. This section explains various RMFs.



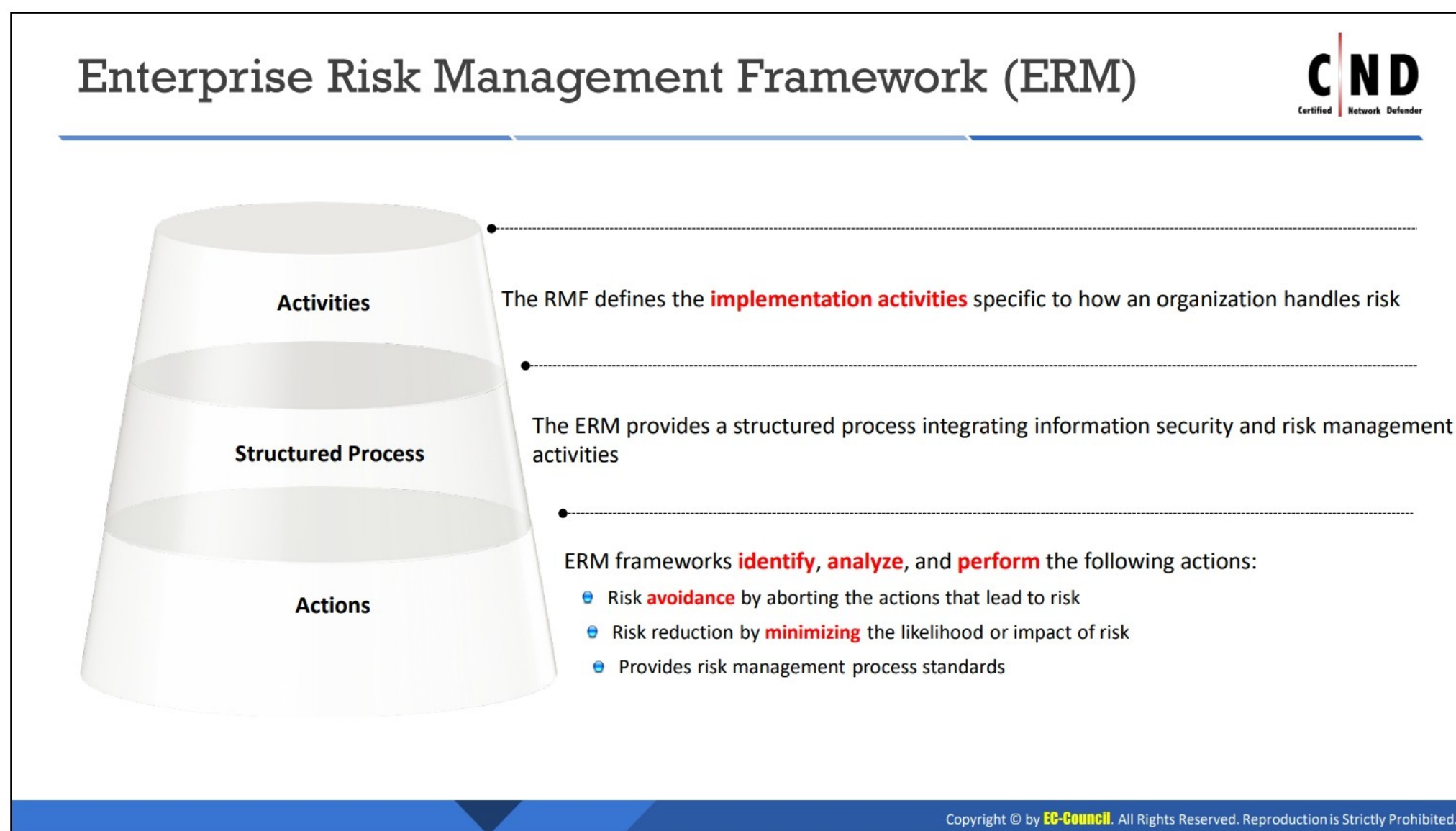


## Enterprise Network Risk Management

Enterprise network risk management attempts to identify, assess, and mitigate threats to the various assets of an organization. It implements a systematic approach to reach the goals and objectives that could satisfy business requirements. It identifies the staff, tools, required skills, and various other resources requires the network defender to

- Identify and understand the current risks;
- Develop procedures to combat network risks;
- Mitigate the various network risks; and
- Develop risk assessment and management policies, procedures, and checklists.





## Enterprise Risk Management Framework (ERM)

Enterprise Risk Management (ERM) includes the methods and processes implemented by an organization to minimize the impact of risks. It involves planning, organizing, leading, and controlling organizational activities to manage risks. ERM can be considered a risk-based approach for managing organizational risks. It provides a framework for risk management that involves

- Identifying events or circumstances relevant to an organization's objectives (risks and opportunities);
- Assessing the identified events for likelihood and magnitude of impact;
- Determining a response strategy; and
- Monitoring process.

The ERM framework helps in identifying and proactively addressing the identified risks. It identifies, analyzes, and performs the following actions:

- Risk avoidance by aborting the actions that lead to risks
- Reducing risks by reducing the likelihood or impact of risks
- Standardizing the risk management process

The key activities involved in managing enterprise-level risk, that is, the risk resulting from the operation of an information system, are as follows:

- Classification of the information system
- Selection of appropriate security controls

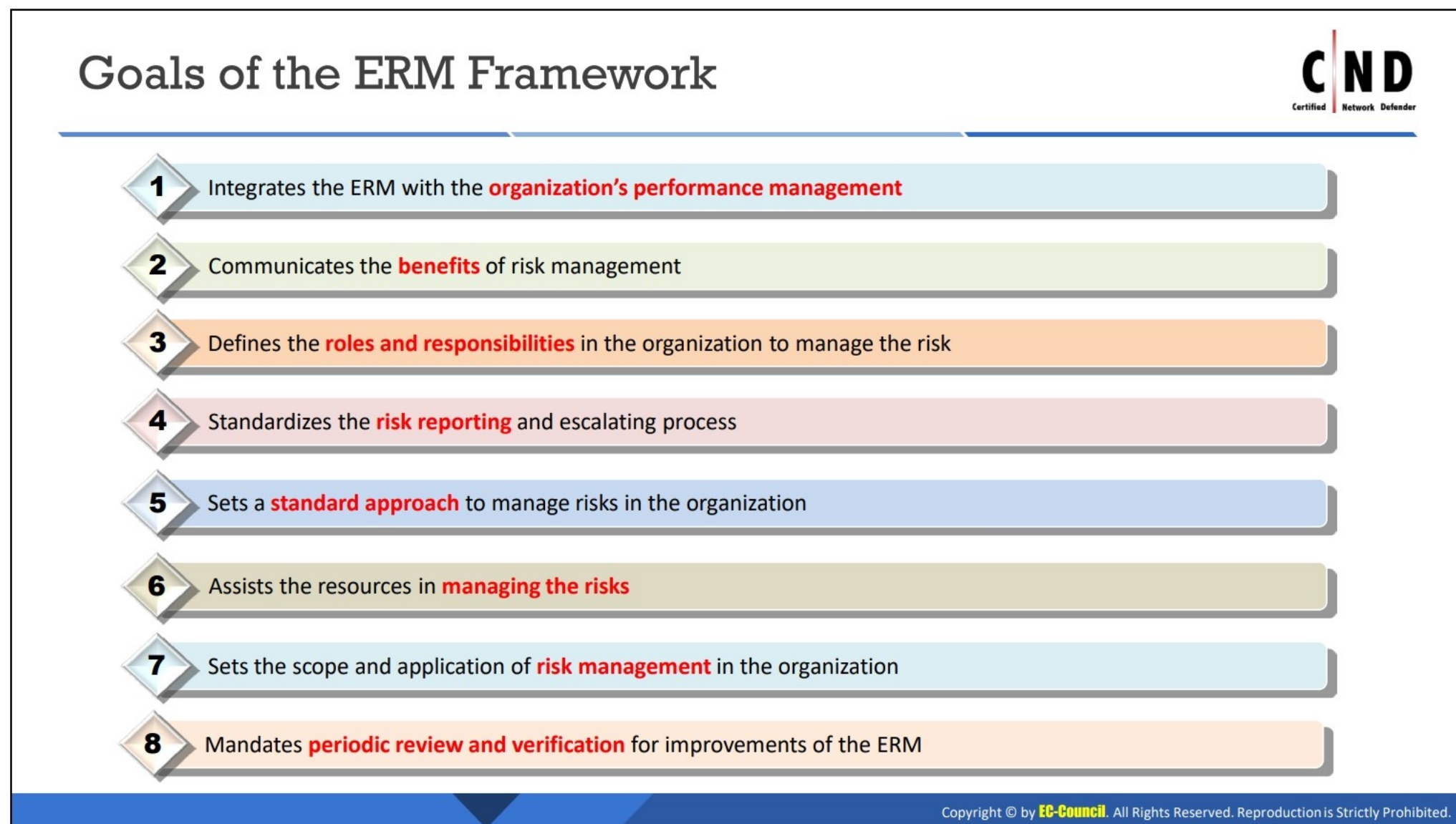


- Refining the selected security control set based on the risk assessment
- Maintaining the document for all selected security controls in a system security plan
- Implementation of the security controls
- Security controls assessment
- Determining agency-level risk and risk acceptability
- Authorizing information system operation
- Monitoring security controls on a continuous basis

This ERM framework helps an organization understand the following:

- Risks coverage
- Risk appetite
- Risk governance (culture, governance, and policies)
- Risk data and infrastructure
- Risks control environment
- Risk measurement and evaluation
- Risks response





## Goals of the ERM Framework

Organizations manage risks and have several departments or risk functions that help in identifying and managing risks. A common goal or the challenge of ERM is improving capability and coordination, while integrating the output to provide a unified picture of risk for stakeholders. The ERM should improve an organization's ability to manage risks effectively.

### Goals of ERM Framework

- Integrate the ERM with an organization's performance management
- Communicate the benefits of risk management
- Define the roles and responsibilities in an organization to manage risks
- Standardize the risk-reporting and escalating process
- Set a standard approach to manage risks in an organization
- Assist the resources in managing the risk
- Set the scope and application of risk management in an organization
- Mandate periodic reviews and verification for improvements of the ERM
- Convey an organization's policies, approach, and attitude toward risk management
- Ensure that an organization should meet risk-reporting commitments



## NIST Risk Management Framework



- NIST RMF is a **structured and continuous process** that integrates information security and risk management activities into the system development life cycle
- **Prepare:** Essential activities to **prepare** the organization to manage security and privacy risks
  - **Categorize:** **Categorize** the system and information processed, stored, and transmitted based on an impact analysis
  - **Select:** **Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
  - **Implement:** **Implement** the controls and document how controls are deployed
  - **Assess:** **Assess** to verify if the controls are in place, operating as planned, and producing the anticipated results
  - **Authorize:** Senior official makes a risk-based decision to **authorize** the system (to operate)
  - **Monitor:** Continuously **monitor** control implementation and risks to the system



NIST Risk Management Framework

Source: <http://csrc.nist.gov>

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

## NIST Risk Management Framework

Source: <https://csrc.nist.gov>

The National Institute of Standards and Technology (NIST) RMF is a set of information security policies and standards for the federal government developed by NIST. It is a structured and continuous risk management process that is integrated into a system development life cycle. The RMF process helps early detection and resolution of risks. It identifies the following processes (tasks) for managing organizational risk, which can be applied to both new and legacy systems:

- **Prepare:** Prepares all levels of the organization by carrying out essential activities to manage security and privacy risks. The outcomes are key risk management and common controls are identified, organization-wide risk assessment is done, organization risk management strategy is established.
- **Categorize:** Categorize the information system and the information processed, stored, and transmitted by a system according to potential worst cases, adverse impact to an organizations mission/business functions, and a system
- **Select:** Select the appropriate baseline security controls based on the categorization in the first step, and implement security controls based on the risk assessment
- **Implement:** Implement security controls and integrate security controls with legacy systems using sound system engineering practices; then apply security configuration settings and document the implemented security controls and their impact on the environment
- **Assess:** Evaluate the implemented security control for effectiveness using appropriate procedures and determine if the controls implemented are working correctly and



effectively; check if they are producing the desired outcome with respect to meeting the security requirements for a system

- **Steps in Assessment**

- Develop the security assessment plan
  - Determine which controls are to be assessed
  - Select appropriate procedures to assess those controls
  - Determine depth and coverage needed for assurance
  - Tailor the assessment procedures
  - Finalize the plan and obtain approval
  - Conduct the assessment
  - Analyze the results
  - Create the security assessment report
- **Authorize:** Determine the risks to organizational operations and assets, individuals, other organizations, and the nation based on the accepted risk appetite with respect to operations and assets (how much risk an organization is willing to tolerate) if acceptable; then, authorize the operation or decide on the required needs
- **Monitor:** Continuously track changes to the information system for signs of attacks that may impact security controls, and regularly monitor the security controls to assess their effectiveness



## COSO ERM Framework



- COSO ERM framework defines essential components, suggests a common language, and provides **clear direction and guidance** for ERM
- COSO framework emphasizes that ERM involves those elements of the management process that enable management to make **genuine risk-based decisions**



Source: <http://www.coso.org>

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

## COSO ERM Framework

Source: <http://www.coso.org>

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was established in the mid-1980s as part of the National Commission on Fraudulent Financial Reporting. It addresses the evolution of ERM and the need for organizations to improve their approach to managing risk to meet the demands of an evolving business environment. It emphasizes considering risk in both the strategy-setting process and driving performance. The COSO ERM Framework consists a set of principles organized into five interrelated components supported by a set of principles.

### COSO ERM Components and Principles

- **Governance and Culture:** Governance sets an organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, ERM. Culture pertains to ethical values, desired behaviors, and an understanding of risk in the entity.
  - **Principles**
    - **Exercises Board Risk Oversight:** The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
    - **Establishes Operating Structures:** An organization establishes operating structures in the pursuit of strategy and business objectives.
    - **Defines Desired Culture:** An organization defines the desired behaviors that characterize the entity's desired culture.



- **Demonstrates Commitment to Core Values:** An organization demonstrates a commitment to the entity's core values.
- **Attracts, Develops, and Retains Capable Individuals:** An organization is committed to building human capital in alignment with the strategy and business objectives.
- **Strategy and Objective-Setting:** ERM, strategy and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
  - **Principles**
    - **Analyzes Business Context:** An organization considers the potential impact of business context on risk profile.
    - **Defines Risk Appetite:** An organization defines risk appetite in the context of creating, preserving, and realizing value.
    - **Evaluates Alternative Strategies:** An organization evaluates alternative strategies and potential impact on the risk profile.
    - **Formulates Business Objectives:** An organization considers risk while establishing the business objectives at various levels that align and support strategy.
- **Performance:** Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. They are prioritized by severity in the context of risk appetite. An organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
  - **Principles**
    - **Identifies Risk:** An organization identifies risks that impact the performance of the strategy and business objectives.
    - **Assesses Severity of Risk:** An organization assesses the severity of risks.
    - **Prioritizes Risks:** An organization prioritizes risks as a basis for selecting responses to risks.
    - **Implements Risk Responses:** An organization identifies and selects risk responses.
    - **Develops Portfolio View:** An organization develops and evaluates a portfolio view of risks.
- **Review and Revision:** By reviewing entity performance, an organization can consider how well the components of ERM function over time and in light of substantial changes, and, thereafter, what revisions are needed.



- **Principles**
  - **Assesses Substantial Change:** An organization identifies and assesses changes that may substantially impact strategy and business objectives.
  - **Reviews Risk and Performance:** An organization reviews entity performance and considers risk.
  - **Pursues Improvement in Enterprise Risk Management:** An organization pursues improvement of the ERM.
- **Information, Communication, and Reporting:** ERM requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across an organization.
  - **Principles**
    - **Leverages Information and Technology:** An organization leverages the entity's information and technology systems to support ERM.
    - **Communicates Risk Information:** An organization uses communication channels to support ERM.
    - **Reports on Risk, Culture, and Performance:** An organization reports on risk, culture, and performance at multiple levels and across the entity.



## COBIT Framework



- **COBIT** is an IT governance framework and supporting **toolset** that allows **managers** to bridge the gap between control requirements, technical issues and business risks
- COBIT **emphasizes** regulatory compliance, helps organizations **increase** the value attained from IT, enables alignment, and simplifies implementation of the enterprise's IT governance and **control framework**



Source: <http://www.isaca.org>

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

### COBIT Framework

Source: <http://www.isaca.org>

Control Objectives for Information and Related Technologies (COBIT) is a framework designed by ISACA for the governance and management of enterprise information (all technology and information processing the enterprise establishes to achieve its goals, regardless of where this occurs in the enterprise) and technology, aimed at the whole enterprise.

COBIT helps enterprises of all sizes

- Maintain high-quality information to support business decisions;
- Achieve strategic goals and realize business benefits through the effective and innovative use of IT;
- Achieve operational excellence through reliable and efficient application of technology;
- Maintain IT-related risk at an acceptable level;
- Optimize the cost of IT services and technology; and
- Support compliance with relevant laws, regulations, contractual agreements, and policies.

### COBIT Framework Internal Stakeholders

- **Risk Management:** Ensures the identification and management of all IT-related risk
- **Assurance Providers:** Manages dependencies on external service providers, provides IT assurance, and ensures an effective and efficient system of internal controls



- **IT Managers:** Provides guidance on how best to build and structure the IT department, manage performance of IT, run an efficient and effective IT operation, control IT costs, and align IT strategy to business priorities.
- **Business Managers:** Helps understand how to obtain the IT solutions that enterprises require and how best to exploit new technology for strategic opportunities
- **Executive Management:** Provides guidance on how to organize and monitor IT performance across the enterprise
- **Boards:** Provides insights on how to obtain value from the use of IT and explains relevant board responsibilities

#### COBIT Framework External Stakeholders

- **IT Vendors'** operations should establish that they are secure, reliable, and compliant with applicable rules and regulations.
- **Business Partners** should confirm that a business partner's operations are secure, reliable, and compliant with applicable rules and regulations.
- **Regulators** should determine whether the enterprise is compliant with applicable rules and regulations, and advise that the enterprise has the right governance system in place to manage and sustain compliance.

#### COBIT Framework Key Concept Principles

- **Governance System Principles:** The six principles are the core requirements for a governance system for enterprise information and technology.
- **Provide Stakeholders Value:** Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of IT.
- **Holistic Approach:** A governance system for enterprise IT is built from a number of components that can be of different types and that work together in a holistic way.
- **Dynamic Governance System:** A governance system should be dynamic. That is, each time one or more of the design factors are changed, the impact of these changes on the EGIT system needs to be considered.
- **Governance Distinct from Management:** A governance system should clearly distinguish between governance and management activities and structures.
- **Tailored to Enterprise Needs:** A governance system should be tailored to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components.
- **End-to-End Governance System:** A governance system should cover the enterprise end-to-end, focusing not only on the IT function, but on all technology and information processing the enterprise puts in place to achieve its goals.



## Governance Framework Principles

- **Based on Conceptual Model:** A governance framework should be based on a conceptual model, identifying the key components and relationships among components, to maximize consistency and allow automation.
- **Open and Flexible:** A governance framework should be open and flexible. It should allow the addition of new content and the ability to address new issues in the most flexible way, while maintaining integrity and consistency.
- **Aligned to Major Standards:** A governance framework should align to relevant major related standards, frameworks, and regulations.

## Governance and Management Objectives

For information and technology to contribute to enterprise goals, a number of governance and management objectives should be achieved. A governance or management objective always relates to one process and a series of related components of other types to help achieve the objective. A governance objective relates to a governance process, while a management objective relates to a management process.

## Goals Cascade

Enterprise goals are consolidated, reduced, updated, and clarified, and, thereafter, alignment goals emphasize the alignment of all IT efforts with business objectives.

## Components of a Governance System

Each enterprise's governance system is built from a number of components. Components can be of different types and interact with each other, resulting in a holistic governance system for IT.

## Focus Areas

A focus area describes a certain governance topic, domain, or issue that can be addressed by a collection of governance and management objectives and their components. Focus areas can contain a combination of generic governance components and variants. The number of focus areas is virtually unlimited, which makes COBIT open-ended. New focus areas can be added as required or when subject matter experts and practitioners contribute. The examples of focus areas include small and medium enterprise, information security, and risk and DevOps.

## Design Factors

Design factors are factors that

- Influence the design of an enterprise's governance system; and
- Position it for success in the use of IT.



## Enterprise Network Risk Management Policy



- Enterprise network risk management policy assists in **developing** and **establishing** essential processes and procedures to address and minimize **information** security risks
- It outlines different aspects of risk and identifies people to manage the risk in the organization

### Objectives:

- Equip the organization with the required skills to identify and treat risks
- Manage the risks with adequate risk mitigation techniques
- Accomplish the strategic and operational goals of the organization
- Provide a consistent RMF
- Combat the existing and emerging risks
- Assist in taking strategic management decisions
- Provide the overall direction and purpose of performing risk management
- Integrate operational risks into the risk management process
- Meet legal and regulatory requirements

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

## Enterprise Network Risk Management Policy

An enterprise network risk management policy is a written statement created to protect an organization's assets from accidental or malicious threats. An organization should ensure they include network risk management policies in their risk management policy that should comply with the security policies of an organization.

Enterprise network risk management policy establishes essential procedures and processes to address and minimize information security risks. This policy addresses information security issues and their impact. It also suggests measures to secure the assets from both internal and external risks.

### Objectives of Enterprise Network Risk Management Policy

- Legal and regulatory adherence
- Strategic management decision assistance
- Achieve organizational strategic/operational goals
- Integrate operational risks into risk management
- Combat existing and emerging risks
- Manage the risks with adequate risk mitigation techniques
- Provide overall direction and purpose for risk management
- Provide a consistent RMF
- Equip an organization with skills to identify and treat risks



## Best Practices for Effective Implementation of Risk Management



✓	Track and monitor <b>internal</b> and <b>external</b> risks of the organization at regular intervals
✓	Establish a <b>risk management policy</b> for the organization
✓	Implement a <b>framework</b> for risk assessment and mapping
✓	Use <b>ERM</b> for decision-making
✓	Incorporate <b>ERM</b> into the strategic planning process
✓	Identify the <b>potential risks</b> to the network
✓	<b>Prioritize</b> the risks based on its impact on the enterprise network
✓	Specify the responsibilities for risk managers with their respective domains
✓	Regularly <b>review</b> and <b>update</b> the risk management policy

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

## Best Practices for Effective Implementation of Risk Management


Implementing ERM involves establishing a proper ERM system.











### Best Practices for Effective Risk Management

- Track and monitor internal and external risks of an organization at regular intervals
- Establish a risk management policy for an organization
- Implement a framework for risk assessment and mapping
- Use ERM for decision-making
- Incorporate ERM into the strategic-planning process
- Identify the potential risks to a network
- Create a common language and reporting system for communicating KRIs
- Prioritize the risks based on its impact on the enterprise network
- Specify the responsibilities for risk management with their respective domains
- Regularly review and update the risk management policy
- Identify the threats and risks arising from user errors and analyze the risks caused in normal and fault conditions
- Always ensure risk assessment is conducted by experienced and trained professionals
- Always identify the risk in its initial stage in order to provide a quick response
- Proper metrics are chosen in order to measure the effectiveness of a risk management system



## ERM Vendors



 <b>Enterprise GRC for Government</b> <a href="http://www.sas.com">www.sas.com</a>	 <b>MetricStream Enterprise Risk Management App</b> <a href="http://www.metricstream.com">www.metricstream.com</a>
 <b>LogicManager Enterprise Risk Management</b> <a href="http://www.logicmanager.com">www.logicmanager.com</a>	 <b>Enablon</b> <a href="https://www.wolterskluwer.com/">https://www.wolterskluwer.com/</a>
 <b>Intelix</b> <a href="http://www.intelix.com">www.intelix.com</a>	 <b>Resolver</b> <a href="http://www.resolver.com">www.resolver.com</a>
 <b>Integrum</b> <a href="http://www.integrumsystems.com">www.integrumsystems.com</a>	 <b>Optial Risk Management</b> <a href="http://www.optial.com">www.optial.com</a>
 <b>STREAM Integrated Risk Manager</b> <a href="http://www.acuityrm.com">www.acuityrm.com</a>	 <b>Cura Risk Management Software</b> <a href="http://www.curasoftware.com">www.curasoftware.com</a>

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

## ERM Vendors

The following are a list of some of the ERM software:

### SAS Governance and Compliance Manager/Enterprise Governance, Risk and Compliance (GRC) for Government

**Source:** [www.sas.com](http://www.sas.com)

The SAS Governance and Compliance Manager or GRC management software gathers information from all financial risk management systems and provides a view of risk exposure throughout the risk management life cycle (risk identification, assessment, monitoring, response, and resolution).

### MetricStream ERM App

**Source:** [www.metricstream.com](http://www.metricstream.com)

MetricStream ERM App enables a systematic process toward managing enterprise risks. Real-time insights into risk management programs are offered through powerful analytics, advanced heat maps, reports, dashboards, and charts.

### LogicManager ERM

**Source:** [www.logicmanager.com](http://www.logicmanager.com)

LogicManager ERM provides a comprehensive matrix of solutions that will accelerate and perfect GRC efforts. It helps develop effective mitigation and monitoring activities as the network defender uncovers the risks across the enterprise.



## **Enablon**

**Source:** [www.wolterskluwer.com](http://www.wolterskluwer.com)

Enablon risk management software is an integrated solution to identify, assess, and mitigate risks across the enterprise. It can

- Manage the impact of uncertainty on an organization's objectives
- Go beyond compliance and gain a competitive edge by improving operational and business performance through effective risk assessments
- Identify and mitigate enterprise and operational risks
- Ensure a consistent approach to risk management

## **Intelex**

**Source:** [www.intelex.com](http://www.intelex.com)

Intelex ERM software allows taking control of both existing and potential risks, integrating risk management into all key organizational processes.

## **Resolver**

**Source:** [www.resolver.com](http://www.resolver.com)

Resolver's risk management software connects risks to incidents. With this connection,

- You can quantify the impact of the risk mitigation plans; and
- Identify where the risk register has gaps and where the risk assessments were overly confident.

This software is aligned to internationally recognized frameworks (including ISO 31000 and COSO ERM) to standardize risk management.

## **Integrum**

**Source:** [www.integrumsystems.com](http://www.integrumsystems.com)

Integrum offers top quality ERM and it is a global leader in risk and quality, health, safety, and environment management.

## **Optial Risk Management**

**Source:** [www.optial.com](http://www.optial.com)

Optial Risk Management allows the identification, assessment, monitoring, and mitigation of risk throughout an organization.



## **STREAM Integrated Risk Manager**

**Source:** [www.acuityrm.com](http://www.acuityrm.com)

The flexible and highly configurable STREAM can quickly automate and improve an organizations' cyber risk management and related integrated risk management applications. It is available as a SaaS or on-premise deployment with support, consultancy, and training services.

## **Cura Risk Management Software**

**Source:** [www.curasoftware.com](http://www.curasoftware.com)

Cura's ERM provides a powerful and flexible framework for managing risk. It allows the identification, analysis, evaluation, and treatment of both risks and opportunities in order to protect an organization.





#### LO#04: Learn to manage vulnerabilities through vulnerability management program

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

### **LO#04: Learn to Manage Vulnerabilities through Vulnerability Management Program**

This section explains how to manage vulnerabilities using a vulnerability management program.



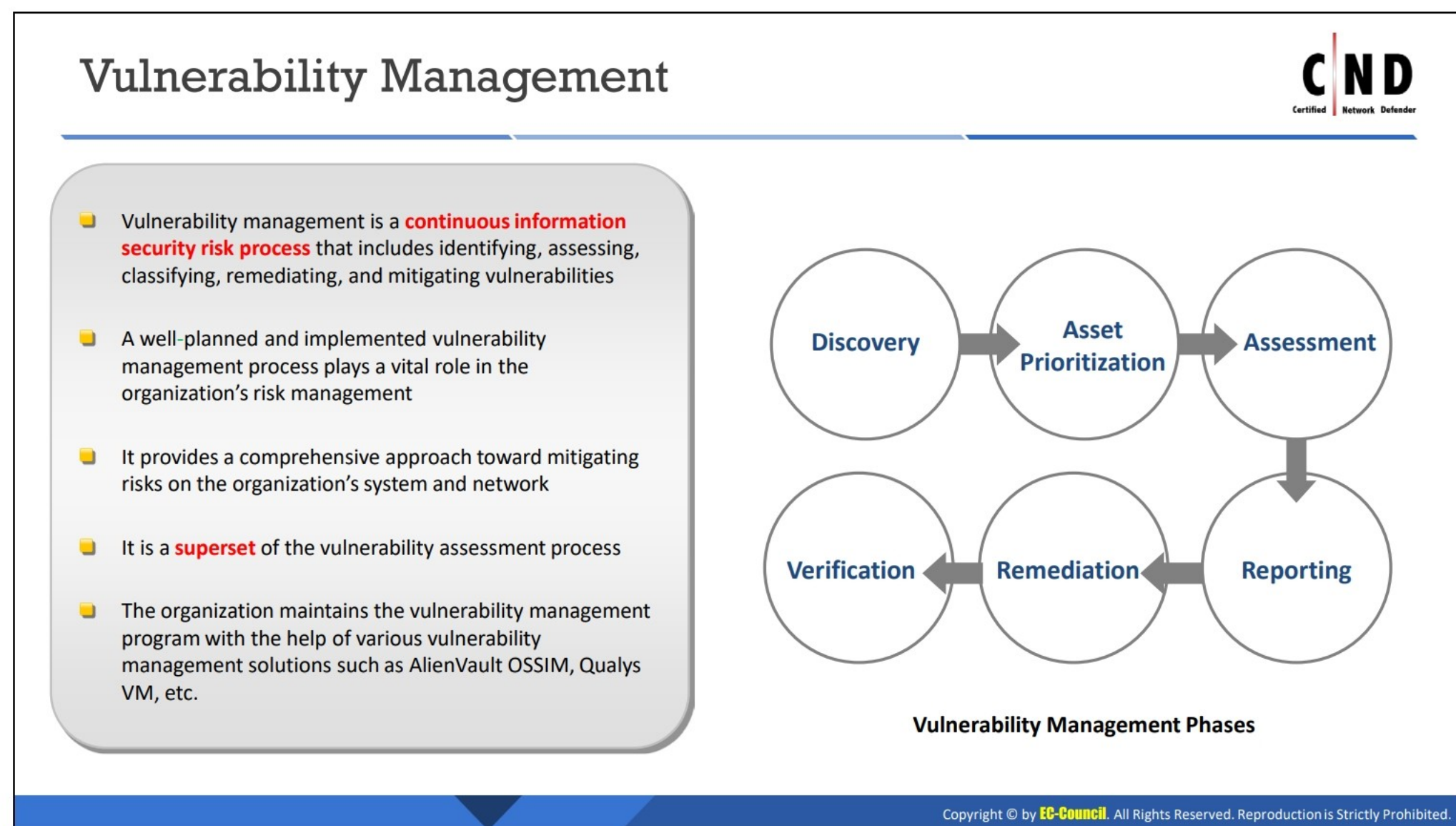


“ The risk management frameworks require organizations to maintain a vulnerability management program”

Source: <http://www.tripwire.com>

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





## Vulnerability Management

Vulnerability management is a continuous information security risk process that includes identifying, assessing, classifying, remediation, and mitigating vulnerabilities. This evaluation helps organizations rectify and remove vulnerabilities or a formal risk acceptance by an organization's management. Well-planned and -implemented vulnerability management can evaluate and control risks and vulnerabilities in a system, playing an important role in an organization's risk management. It provides a comprehensive approach toward mitigating risks in an organization's system and network.

Vulnerability management is usually confused with vulnerability scanning or identification. Vulnerability scanning (e.g., scanning to identify vulnerabilities in networks, systems, and applications) is executed by using a vulnerability scanner, while vulnerability management is the process in vulnerability scanning in addition to risk acceptance and remediation, among others. Vulnerability assessment is a part of vulnerability management.

Some of the most popular vulnerability management solutions that help organizations maintain their vulnerability management programs are AlienVault Open Source Security Information and Event Management System, Qualys Virtual Machine, Rapid 7, McAfee, and Tenable Network Security.

There are six phases in vulnerability management. Every process focuses on improving the security risks of a network:

- **Discovery (Mapping):** Identify, consider, and evaluate a network asset
- **Asset Prioritization (and Allocation):** Compare risks against a predefined set of features and assign priorities



- **Assessment (Scanning):** Scan and evaluate a system for vulnerabilities
- **Reporting (Technical and Executive):** Report the results for the different vulnerability management processes
- **Remediation (Treating Risks):** Reduce the risks and remove the root cause
- **Verification (Rescanning):** Monitor network continuously to check for new vulnerabilities



## Discovery: Identify the Assets and Components of a Network

In this phase, all network components and assets are **identified**

Assets identification will help you detect **rogue** devices (if any) on the network

It provides a **hacker's view** of the network

The screenshot shows the OSSIM Asset Discovery web interface. The 'ASSETS' tab is selected under 'ASSETS & GROUPS'. The 'SCAN FOR NEW ASSETS' section shows a 'TARGET SELECTION' dropdown with 'All Assets' selected. Below this, there are options for 'Local sensor' and 'Automatic sensor'. The 'ADVANCED OPTIONS' section includes 'Scan type' (Full Scan), 'Timing template' (Normal), and checkboxes for 'Autodetect services and Operating System' and 'Enable DNS Resolution'. The 'SCAN RESULTS' table at the bottom lists discovered assets with columns for Host, Hostname, IPQDN, Device Types, MAC, OS, and Services. The table shows three entries: 10.10.10.16 (Windows 2016), 10.10.10.2 (Windows Longhorn), and 10.10.10.75 (Ubuntu 3.X).

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

## Discovery: Identify the Assets and Components of a Network

Identifying the assets and various components of a network is the first phase of the vulnerability management. An inventory that details the inactive and active assets and network components should include the physical and logical elements of the information infrastructure to identify the vulnerabilities. Assets include hardware devices such as servers, internal applications, and software licenses. The discovery process should comprise the location, business processes, data classification, identified threats, and risks for every element. Having a better idea about assets allows a clear picture of the relationship between the assets and network components.

### Functions of Discovery Phase

- Identifies all hosts (including rogue devices) in a network and assigns the host according to the business needs
- Provides a graphical representation of the hosts in a network
- Performs a risk-based approach in ranking the remedial efforts
- Identifies services and ports, for example, running on each identified device
- Selects preferred hosts for scanning or reporting
- Provides a hacker's view of a network

Use automated network discovery tools to identify a network component. An automated scheduled check for vulnerabilities can be performed. Security information and event management can automatically discover all assets attached to a network. For example, AlienVault OSSIM Asset Discovery helps perform asset discovery, which provides information about



- All assets in cloud solutions and on-premises environments; and
- Internet provider (IP)-enabled devices on a network, which decides what software and services are installed on them and how they are configured.

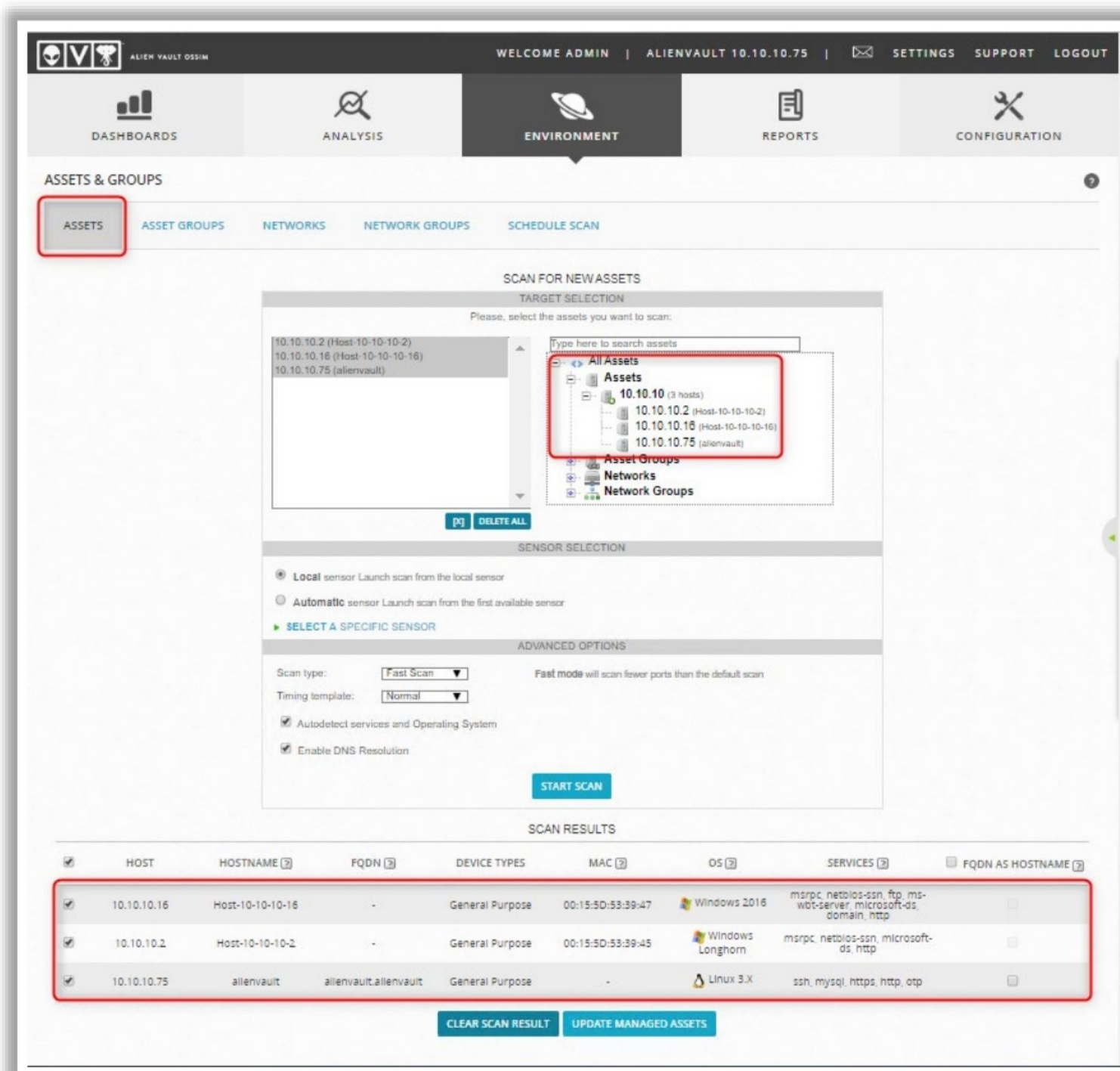


Figure 18.1: OSSIM Asset Discovery



## Asset Prioritization: Evaluate the Importance of Each Component



### OSSIM Asset Prioritization

- Asset prioritization helps create a **customized list** of what to tackle first, second, third, and so on
- Identify the assets that are more **critical** to the business
- Identify the **value** for each specific asset
- Criticality of the assets depend on the business impact

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

## Asset Prioritization: Evaluate the Importance of Each Component

All assets do not have the same significance. The network defender needs to classify the identified assets according to business needs. This helps identify the high business risks in an organization. Prioritize the assets based on the impact of their failure and on the reliability of those assets in the business. Thus, prioritization helps

- Create a customized list of what to tackle first, second, third, and so on;
- Identify the assets that are more critical to the business;
- Identify the value for each specific asset;
- Evaluate and decide a solution for the consequence of the assets failing;
- Examine the risk tolerance level; and
- Organize the methods for prioritizing the assets.

Prioritize assets by assigning different values to the assets. The asset's value and the information the asset can access should be correlated with the possible vulnerabilities. After correlation, every asset–vulnerability pair should be clubbed with a known threat. These three values should provide an idea of which assets and risks to prioritize in the vulnerability management process. For example, in the AlientVault's USM Appliance, the network defender can set the asset value to prioritize the assets by giving it a value between 0 and 5, where 0 indicates least importance and 5 indicates the most important.

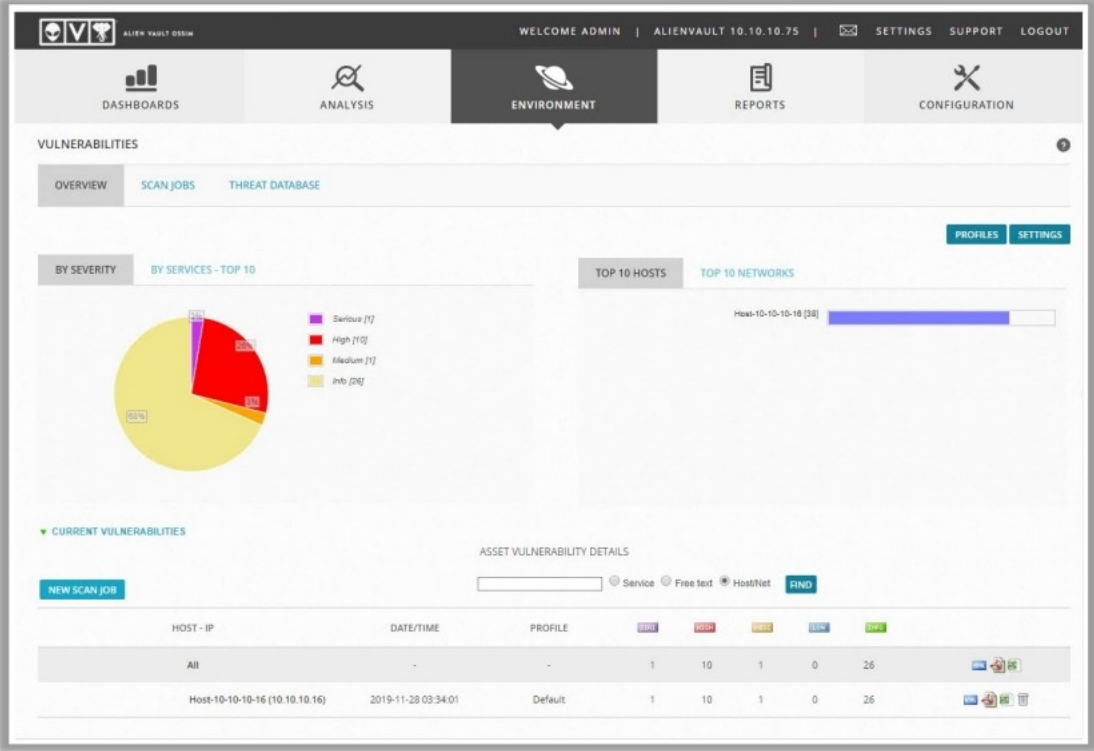


The screenshot shows the 'NEW ASSET' form in the AlienVault OSSIM interface. The form includes fields for Name, IP Address, FQDN/Aliases, Location, Asset Value, External Asset, Latitude/Longitude, Operating System, Model, Description, and Sensors. The 'Asset Value' dropdown is highlighted with a red box and a callout. The callout text states: 'You can prioritize your assets by assigning asset value to them, assign asset value ranging from 0 to 5, 0 being the least important and 5 the most important'. The 'Asset Value' dropdown is currently set to 5. The 'Operating System' field is set to 'Microsoft Windows Server 2016'. The 'Model' field is empty. The 'Description' field is empty. The 'Sensors' field is set to '10.10.10.75 (alienvault)'. The 'External Asset' field is set to 'No'. The 'Latitude/Longitude' field is empty. The 'Location' field is empty. The 'FQDN/Aliases' field is empty. The 'IP Address' field is set to '10.10.10.16'. The 'Name' field is set to 'Web Server'. The 'Icon' field is empty. The 'Choose icon ...' button is visible. The 'SAVE' button is at the bottom right of the form.

Figure 18.2: OSSIM Asset Prioritization



## Vulnerability Assessment



Report the vulnerabilities discovered to the **security team, auditors, and management**

Reports include a **prioritization** matrix for all discovered assets and vulnerabilities

Reports include a risk summary, consolidated vulnerability list, exploit results, and network device details

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

## Vulnerability Assessment

A vulnerability assessment is the process of identifying vulnerabilities in network components, including the OS, web applications, and web servers. It helps identify the category and criticality of the vulnerability in an organization. An organization rates the vulnerabilities and prioritizes them, and design methods to remedy the situation accordingly. The assessment method helps measure the effectiveness of those remedies. The goal of the vulnerability assessment includes scanning, examining, evaluating, and reporting the vulnerabilities in a network to, thus, minimize the levels of risks to an organization.

Vulnerability assessment is a key element of a vulnerability management framework. It is considered the first step for enhancing IT security and has multiple benefits.

### Benefits of Vulnerability Assessment

- Identifying the key information assets of an organization
- Deciding the vulnerabilities that threaten the security of those assets
- Providing recommendations to strengthen the security posture
- Mitigating risks

### Steps in Vulnerability Assessment

- Classify a network or system resources
- Prioritize the importance of each resource
- Identify the possible threat to each resource
- Identify the possible measures for each threat



- Identify the methods required to reduce the impact of any attack

### Advantages of Vulnerability Assessment

- Identifies known security issues before potential attackers find the vulnerability and exploit it
- Provides the opportunity to address the issues and avoid serious damage to an organization's assets
- Assists in updating or creating a detailed structure of an organizations network
- Identifies rogue machines on a network and avoids unnecessary risks to an organization
- Helps create an inventory of network resources that are useful when tracking systems
- Assists organizations in generating a blueprint of its overall security posture
- Reduces liability and protects assets
- Identifies issues on systems that security controls are unable to identify
- Alerts security managers when an attack occurs
- Provides additional assurance to security managers on the state of the security system

Use scheduled vulnerability assessments of the environment to assess known vulnerabilities based on the security configuration policies that are defined for that environment.

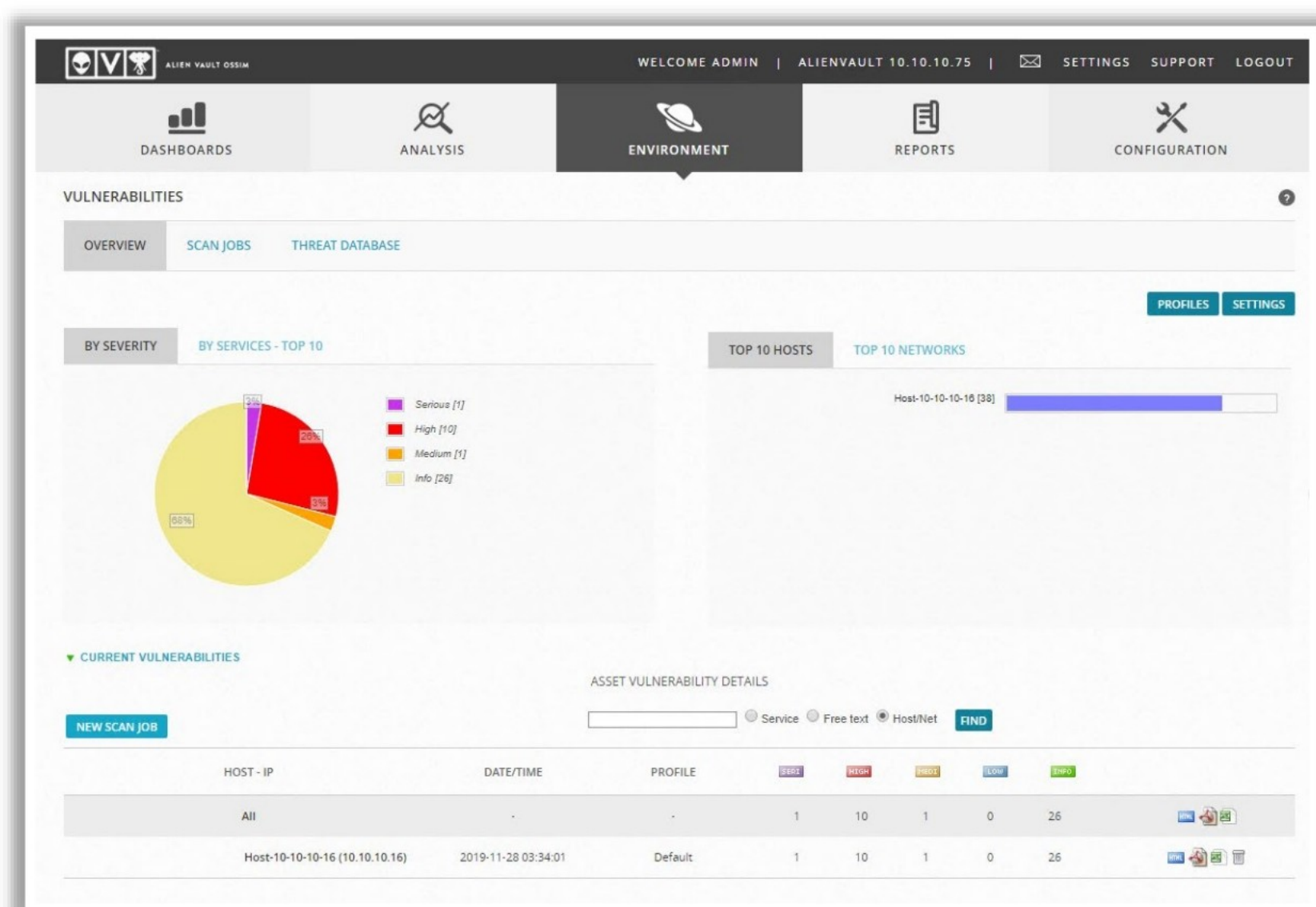



Figure 18.3: OSSIM Vulnerability Assessment



## Mitigation



- It is an action taken to prevent vulnerabilities from **exploitation**
- Reduces the risk by taking other actions, instead of **correcting** a discovered vulnerability
- For example,**
  - Installing a web application firewall is a mitigation action for a discovered web application vulnerability, instead of fixing the vulnerability

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

## Mitigation


Mitigation involves minimizing the risk of a vulnerability by performing certain actions. It can be improved by recognizing and categorizing the risks in accordance with the business operations. Mitigation measures can eliminate or reduce the risk of a vulnerability completely. Network defenders should, thus, use appropriate mitigation strategies and techniques based on the vulnerability encountered.

### Types of Mitigation Actions

- Installing a web application firewall to mitigate discovered web application vulnerabilities
- Organizing a transit access control list: Allowing only authorized traffic to pass through the access points or by allowing the traffic at access points according to certain policies and procedures
- Provide spoofing protection:
  - **Unicast Reverse Path Forwarding (URPF):** It protects the packets in a network from spoofing; a proper URPF mode should be configured before enabling this feature
  - **IP Source Guard:** It prevents IP traffic on non-routed and layer 2 interfaces by classifying packets



## Remediation



Remediation is the process of **correcting** a discovered vulnerability

**Remediation Steps:**

- Ensure whether the vulnerability found is a **false positive** or a **real vulnerability**
- Develop a remediation plan to fix the identified vulnerability
  - **E.g.**, applying appropriate patches to fix the vulnerability
- Remediate a vulnerability by executing the steps in a remediation plan

**Remediation plan should include:**

- Actions for fixing, mitigating, or accepting vulnerabilities
- Mode of remediation (automatic or manual)
- Action for mitigating any remaining vulnerabilities
- Justification for accepting any vulnerability

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

## Remediation

Remediation is the process of fixing identified vulnerabilities. Network defenders should create a remediation plan and implement it to eradicate such vulnerabilities. They should have a phased remediation strategy to address the vulnerability landscape. Remediation may range from applying technical security measures at the host level to a network level.

### Remediation Step

- Confirming the created remediation is not based on a false positive
- Creating a prioritized list for remediation
- Creating a remediation plan to repair the vulnerability
- Remediate the vulnerability by implementing steps in the remediation plan

Certain deadlines are set in order to complete the remediation process. The remediation timeframe should be in accordance with the identified risk level.

### Guidelines for Remediation


- Proper tools should be implemented for vulnerabilities, and an organization should approve the tools before they are implemented.
- Remediation should improve the efficiency of the process. Automation of the process improves the functioning of the process.

### Types of Remediation Tasks

- Action Plan:** Budget, resources, priority, timing (e.g., immediate, 30 days, 6 months, and future)
- Typical Actions:** Patch, upgrade, configuration standards rollout (by role), infrastructure refresh, and new deployment



## Verification



- Perform another scan to ensure the vulnerability is **fixed** after the remediation process
- Verifying the fixes ensure **compliance** with security
- The verification should not **damage** any other network devices, services, or applications

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

## Verification

Verifying the remediation ensures the vulnerabilities have been solved and fixed appropriately. After finishing the remediation process, the network defender should scan for the vulnerability again and perform an unlimited scan for all vulnerabilities that were originally discovered. The vulnerability assessment will close upon verification of a successful remediation. Verification should not lead to the malfunction of any other network device, service, or application. The vulnerability scan reports obtained after the fixes were verified ensures compliance with security provisions.



## Additional Vulnerability Management Solutions



Source: <https://www.qualys.com>

**InsightVM**  
<https://www.rapid7.com>

**ManageEngine Vulnerability Manager Plus**  
<https://www.manageengine.com>

**BeyondTrust Vulnerability Management**  
<https://www.beyondtrust.com>

**Skybox Vulnerability Control**  
<https://www.skyboxsecurity.com>

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

## Additional Vulnerability Management Solutions

### Qualys Vulnerability Management

Source: [www.qualys.com](http://www.qualys.com)

Qualys' Vulnerability Management can continuously detect and protect against attacks anytime and anywhere.

### InsightVM

Source: [www.rapid7.com](http://www.rapid7.com)

InsightVM allows network defender to find, prioritize, and remediate vulnerabilities. It is recognized as a leader in the Forrester Wave™: Vulnerability Risk Management, Q4 2019.

### ManageEngine Vulnerability Manager Plus

Source: [www.manageengine.com](http://www.manageengine.com)

Vulnerability Manager Plus delivers comprehensive vulnerability scanning, assessment, and remediation across all endpoints in a network from a centralized console.

### BeyondTrust Vulnerability Management

Source: [www.beyondtrust.com](http://www.beyondtrust.com)

BeyondTrust Vulnerability Management mitigates the risks with cross-platform vulnerability assessment and remediation, including built-in configuration compliance, patch management, and compliance reporting.



## **Skybox Vulnerability Control**

Source: [www.skyboxsecurity.com](http://www.skyboxsecurity.com)

The Skybox Vulnerability Control provides risk-based vulnerability prioritization and scan-less vulnerability assessment. It removes blind spots and shows how vulnerabilities and threats could impact the system.





## LO#05: Learn vulnerability scanning and assessment


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

### **LO#05: Learn Vulnerability Scanning and Assessment**

This section explains how to perform network and web application vulnerability assessments.



## External Network Vulnerability Assessment



- External vulnerability scanning **examines** an organization's network security from the **outside**
- It involves identifying the vulnerabilities in operating systems, devices, and applications on the Internet-facing hosts

Execute the following steps to conduct an effective external network vulnerability assessment:

- Find the live hosts on a network
- Perform OS fingerprinting on the detected hosts
- Detect open ports on the target system
- Map open ports and running services
- Find the version of all running services
- Map the service version with the security vulnerabilities which are associated
- Check if the service is vulnerable or if it has been patched

```
root@alice-Virtual-Machine: /home/alice
root@alice-Virtual-Machine: /home/alice# nmap -sV -T4 -f www.certifiedhacker.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-08 04:38 EST
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.086s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 975 filtered ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Pure-FTPd
22/tcp    open  ssh            OpenSSH 7.4 (protocol 2.0)
23/tcp    closed telnet
25/tcp    open  smtp           Exim smtpd 4.96.2
80/tcp    open  http           Apache httpd
110/tcp   open  pop3           Dovecot pop3d
119/tcp   closed nntp
143/tcp   open  imap           Dovecot imapd
443/tcp   open  ssl/http       Apache httpd
465/tcp   open  ssl/smtp       Exim smtpd 4.96.2
563/tcp   closed snews
587/tcp   open  smtp           Exim smtpd 4.96.2
993/tcp   open  ssl/imap       Dovecot imapd
995/tcp   open  ssl/pop3       Dovecot pop3d
1863/tcp  closed msnp
5050/tcp  closed mmcc
5190/tcp  closed aol
```

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

## External Network Vulnerability Assessment

An external vulnerability assessment evaluates the security profile of an organization from a network perimeter. It assists in the identification of network vulnerabilities.

### Actions in External Vulnerability Assessment

- Find all hosts on a network
- Fingerprint their OSes
- Detect open ports on a system
- Map the ports to various network services
- Detect the version of all running services
- Map the service version to the discovery of any security vulnerabilities
- Verify if the service is vulnerable to an attack or if it has been patched

### Examples of External Vulnerabilities

- FTP Anonymous Access:** A review of the perimeter security, whether the server permits terminated employee accounts anonymous access to files and services
- Email Relay:** Checking whether the email server allows open email relaying



## **Four Stages of Vulnerability Assessment**

- Plan and configure the vulnerability assessment
- Set up the tasks to run and generate the reports
- Resolve the vulnerabilities
- Maintain a security baseline for a network

## **Guidelines for Effective External Vulnerability Assessment**


- Regularly perform an external vulnerability assessment: The assessment includes all devices in a network, including new ones. Vulnerabilities detected in one device or a system do not mean the entire network is corrupt. However, the need to optimize a network security increases.
- Assess and analyze the hardware manufacture, procurement, storage, and installation: Find the devices that are non-functional or non-compatible with the infrastructure. Detect all open ports and interfaces and act accordingly.
- Avoid conducting a vulnerability assessment on a particular device or a system: The vulnerability assessment should be applicable for all devices in a network. Determine the status of the services running on a system. Unpatched applications can be vulnerable to attacks. Patch any application or service that is not patched and requires an update.
- Map a network infrastructure, connecting the hardware together to boost the network and application performance.

## **Typical Tasks for Effective External Vulnerability Assessment**

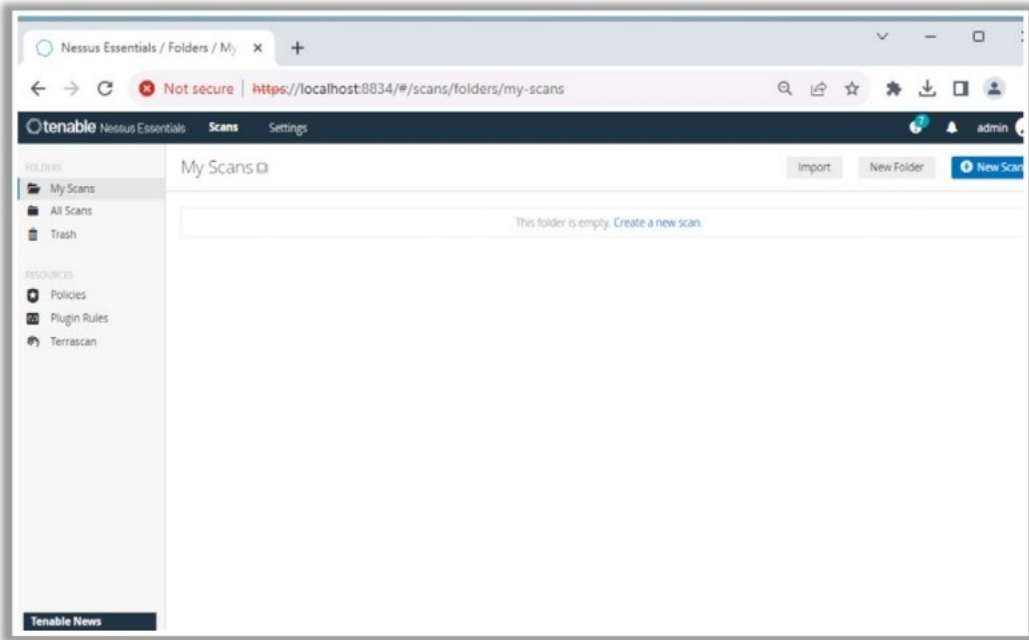
- Collect all information related to a network
- Collect and document all information, including that available on the public facing network; this allows authorities to detect any possible way an attacker may infiltrate a network
- Conduct network application probing and scanning
- Conduct OS fingerprinting and vulnerability detection to locate the vulnerable hosts
- Evaluate the findings and reports for a detected vulnerability to perform the necessary actions
- Identify all weak user authentication systems




## Internal Network Vulnerability Assessment





- Internal vulnerability assessments help identify vulnerabilities within the network including password complexity, antivirus protection, and other potential weaknesses
- Use **network vulnerability scanning tools** such as Nessus to scan your network for vulnerabilities



### Additional Network Vulnerability Scanning Tools

**GFI LanGuard**  
<http://www.gfi.com>

**OpenVAS**  
<http://www.openvas.org>

**Nsauditor**  
<http://www.nsauditor.com>

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

## Internal Network Vulnerability Assessment

An internal network vulnerability assessment recognizes the vulnerabilities such as password complexity and antivirus protection used in a network. An internal assessment evaluates a network for the presence of internal vulnerabilities. Conduct a vulnerability assessment on every critical device to identify all possible vulnerabilities that an attacker could exploit. Internal assessments create a report based on the vulnerabilities detected in a network. The internal vulnerability assessment includes:

- **Host and Service Discovery:** Discovering all accessible systems and services running, which includes live host detection, service enumeration, and application fingerprinting
- **Vulnerability Identification and Verification:** Vulnerability scans are performed on a discovered host and the services in order to identify any vulnerabilities present

### Examples of Internal Vulnerabilities

- **Ineffective Procedures:** Ineffective security configuration procedures in a network
- **Old Passwords:** Includes passwords older than one month
- **Old Patch Levels:** Old versions of patches and updates
- **Unnecessary Services:** Multiple ports open indicating the presence of unnecessary server services



## **Additional Vulnerability Scanning Tools**

### **GFI LanGuard**

Source: <https://www.gfi.com>

GFI LanGuard is compatible with Microsoft®, Mac OS X®, and Linux® OSes as well as many third-party applications. Scan the network automatically or on demand. The GFI LanGuard network security scanner can identify more than 60,000 vulnerabilities. It scans devices, identifies, and categorizes security vulnerabilities, and then recommends a course of action and provides the network defender with the tools to solve the problem. The graphic threat level indicator provides an intuitive, weighted assessment of the vulnerability status of scanned devices.

### **OpenVas**

Source: <http://www.openvas.org>

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated testing, authenticated testing, various high- and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any type of vulnerability test.


### **Nsauditor**

Source: <http://www.nsauditor.com>

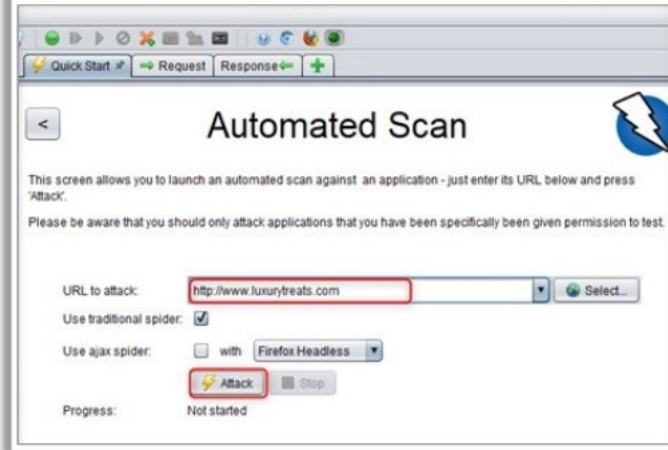
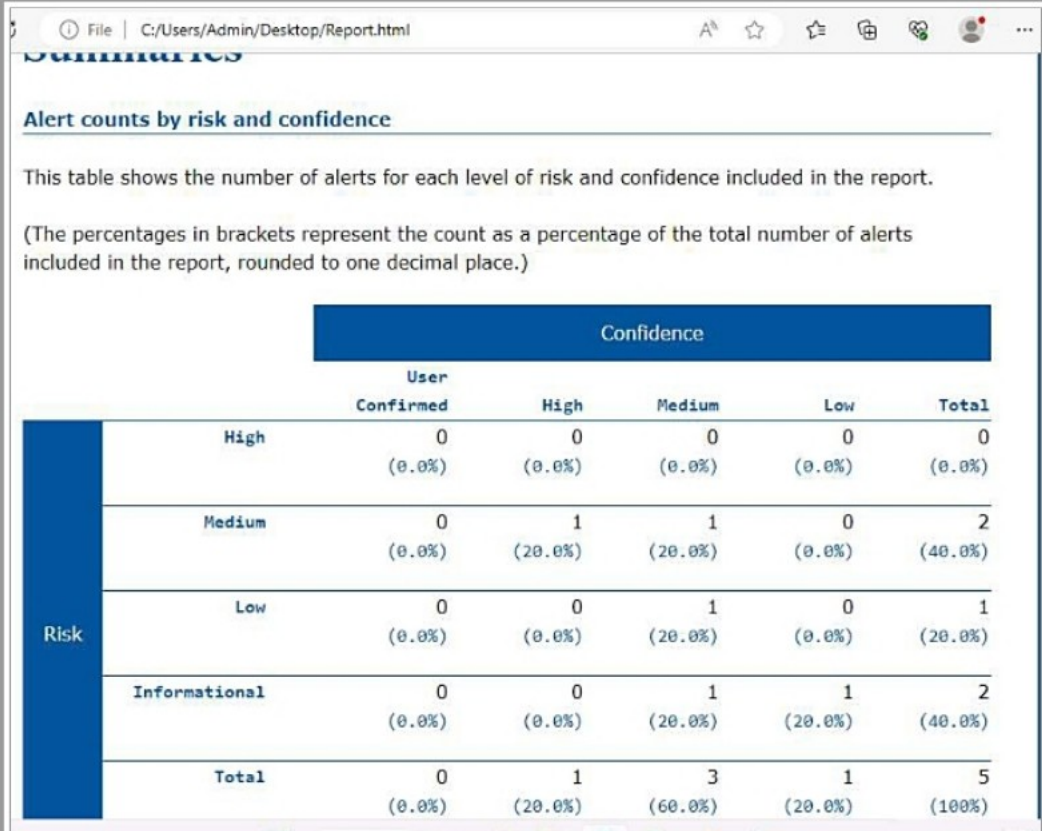
Nsauditor is the best network security auditing tools suite; it includes more than 45 network tools and utilities such as for network security auditing, network scanning, and network monitoring. Its Network Security Auditor is a powerful network security tool designed to scan networks and hosts for vulnerabilities, and to provide security alerts.



## Web Vulnerability Assessment



Run Web Application Vulnerability Scanners such as OAWSP ZAP, WebInspect, IBM Security AppScan, Qualys, Vega, etc. to **scan web applications** for vulnerabilities

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

## Web Vulnerability Assessment

Web vulnerability assessment involves crawling the website in order to discover potential vulnerabilities, and then report these results. There are many open source and commercial vulnerability scanning tools to perform such an assessment. The main here is to make websites vulnerability free. The following vulnerability assessment functions are crucial when selecting a web application vulnerability scanner:

- User-friendly interface
- Automated assessment processes
- Easily assign priorities and grouping
- Accurate Reports

## Web Application Vulnerability Scanners

### OWASP ZAP

Source: <https://www.owasp.org>

OWASP ZAP is an open source, easy to use, integrated tool for finding vulnerabilities in web applications.

### WebInspect

Source: <https://www.microfocus.com>

HP WebInspect is a web application security assessment solution designed to thoroughly analyze complex web applications and services for security vulnerabilities. It provides the broadest



dynamic application security testing coverage and detects new types of vulnerabilities that often go undetected by black-box security testing technologies.

### **IBM Security AppScan**

Source: <https://www.ibm.com>

IBM Security AppScan® Standard is a security vulnerability testing tool for web applications and services. It features the most advanced testing methods to help protect a site from cyber-attacks, together with a full range of application data output options.

### **Qualys Web Application Scanner**

Source: <https://www.qualys.com>

Qualys is a robust cloud solution for continuous web app discovery and detection of vulnerabilities and misconfigurations.

### **Vega**

Source: <https://subgraph.com>

Vega vulnerability scanner is an open source web security tool to test the security of web applications. It can help find and validate SQL injections, cross-site scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities.





---

## LO#06: Discuss Privacy Impact Assessment (PIA)

---

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

### **LO#06: Discuss Privacy Impact Assessment (PIA)**

This section explains Privacy Impact Assessment and its process.

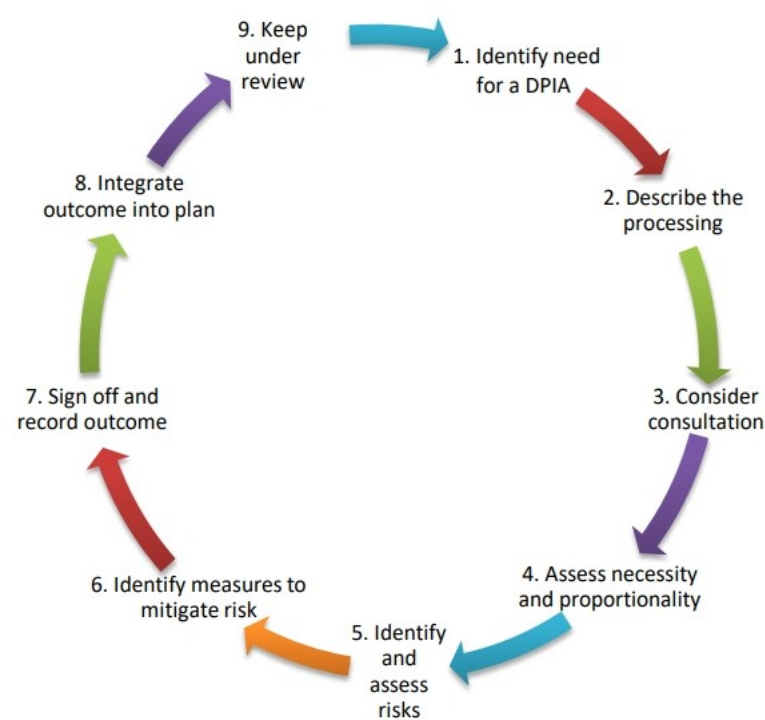


## What is Data Protection Impact Assessment (DPIA)



- The data protection impact assessment (DPIA) process is a **structured and systematic** approach that organizations follow to assess and manage the privacy risks associated with specific data processing activities

- The process is essential for compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) and is **designed to protect** the rights and freedoms of individuals whose personal data is being processed



Steps to Conduct Data Privacy Impact Assessment

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

### What is Data Protection Impact Assessment (DPIA)

The Data Protection Impact Assessment (DPIA) process is a structured and systematic approach that organizations follow to assess and manage the privacy risks associated with specific data processing activities. The process is essential for compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), and is designed to protect the rights and freedoms of individuals whose personal data is being processed.

#### Steps to Conduct Data Privacy Impact Assessment

- **Identify the need for DPIA:** In this step, finish the DPIA initial screening to determine whether the organizations needs to complete a DPIA. In a DPIA template, list the types of processing identified in the screening, aim of the DPIA, and why the need to finish DPIA was identified.
- **Describe the processing:** In this step, the organization must decide the data to be processed, various data resources, the level of access to it, the risk involved with it, and how much of the processing will be done, why it will be done, and in what context.
- **Consider consultation:** In this step, consult the stakeholders at different levels to seek their views and determine the requirement to include third-party expertise consultation.
- **Assess necessity and proportionality:** In this step, assess whether the chosen model can help the organization achieve the expected outcome and evaluate the steps needed to examine the quality of data. In the case of AI, organizations must design steps to eliminate biases.



- **Identify and assess risks:** In this step, ensure that the model does not pose any risk such as intrusion into private spaces, access to unauthorized assets, violation of regulations and compliances, access to websites that have age and content restrictions, financial harmful activities, etc.
- **Identify measures to mitigate risk:** In this step, suggest the mitigation measures to the risks and hams that are identified in the previous step. Determine the effect and severity of risk on the organization's assets.
- **Sign off and record outcomes:** In this step, submit the assessment as feedback on whether the process is compliant and can go ahead. Record reasons if decide not to follow anyone's advice.
- **Integrate outcomes into the plan:** In this step, integrate the outcomes of DPIA back into the plan. Identify action points and the responsibility of implementing those action points.
- **Keep under review:** In this step, review the DPIA. Repeat the DPIA processing if substantial changes are found to the nature, scope, context, or purpose of it.



## What is Privacy Impact Assessment (PIA)?



- Privacy impact assessment (PIA) is a process designed to identify and address **data protection risks** within a new or existing project

### PIA Primary Objectives

- Compliance with **suitable policies** and legal and regulatory requirements are ensured
- Detect and determine the **cyber risks** and their **impact in privacy**
- Evaluate and practice additional methods and approaches to **mitigate** potential privacy risks

### PIA is Conducted When

- New technologies** are adapted and developed to handle PII
- Designing fresh data or information that could pose a **heavy risk**
- Updating a system that could introduce **new risks**
- Implementing or revising new rulemaking that involves **PII gathering**

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

## What is Privacy Impact Assessment (PIA)?

A Privacy Impact Assessment (PIA) is a risk assessment procedure that examines the processes that address data protection risks involved in an information system and identifies privacy risks associated with an organization's confidential information. It offers insights into notable deficiencies within the privacy department, compliance, and risk management. Implementing PIA either prevents or mitigates risks thereby enhancing privacy protections. It explains the purpose of collecting personally identifiable information (PII), how the collected information is maintained, and how it will be protected, and how it will be retained.

A PIA should achieve three primary objectives:

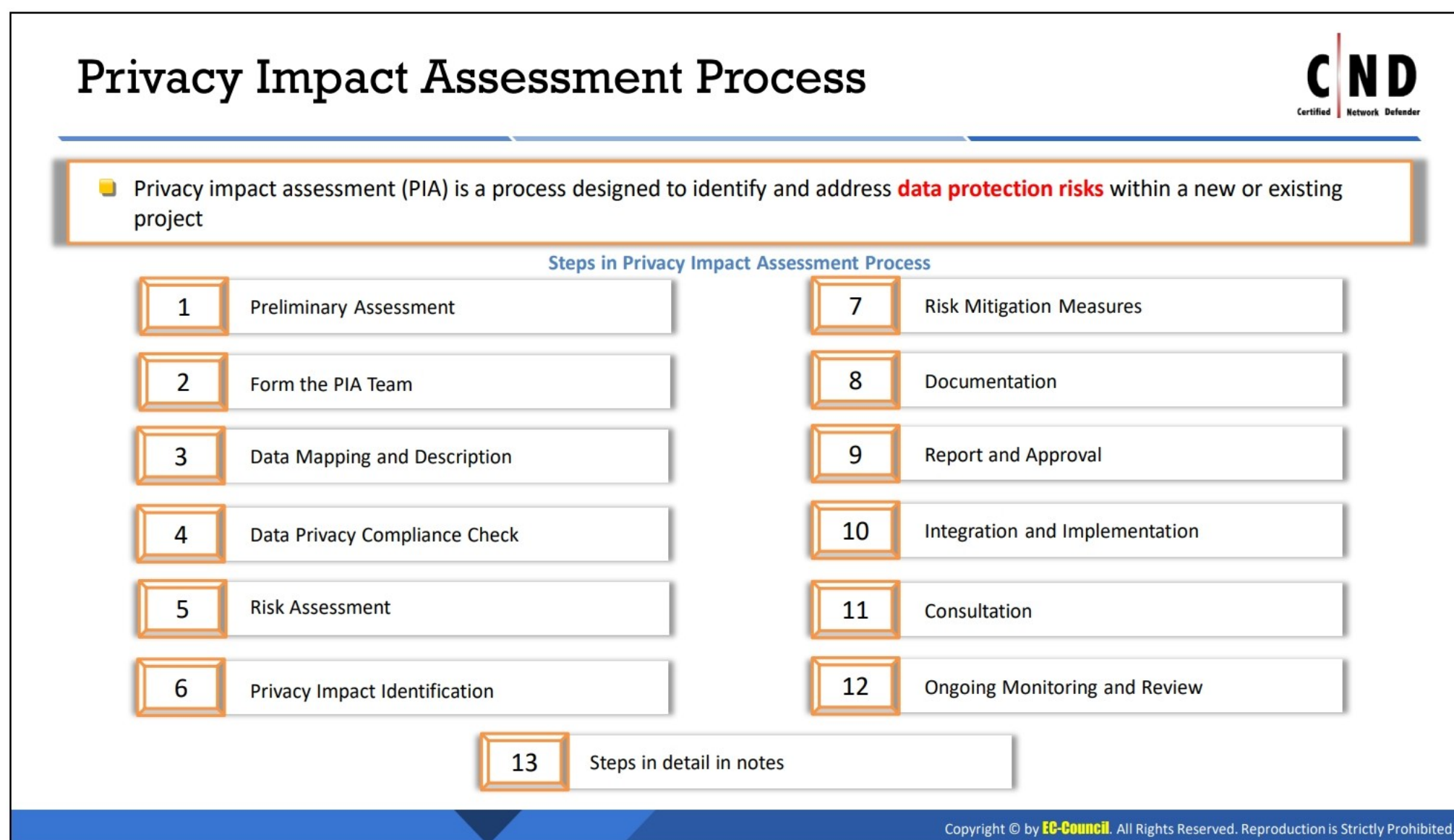
- Ensure adherence to relevant legal, regulatory, and policy requirements for privacy.
- Identify and address the risks of privacy breaches and their effects.
- Assess alternative processes and protections to mitigate potential privacy risks.

Information is a very important asset for an organization and safeguarding it is necessary. Implementing PIA offers risk management capabilities for an organization. An efficient PIA ensures compliance and identifies and addresses privacy issues. PIA is required to be conducted to determine whether the project involves PII, and if so, how the information that is collected is secured. Organizations should conduct PIAs whenever there is a potential risk to an individual's personal information due to a program or activity.

PIA is conducted in case of the following situations:

- When developing/procuring new technologies that take care of PII
- When creating a new information collection system that may have privacy risks
- When updating an information system that may have new privacy risks
- When issuing a new or updated rulemaking that involves collecting PII





## Privacy Impact Assessment Process

A Privacy Impact Assessment (PIA) is a systematic process used to identify and assess the potential privacy risks and impacts associated with specific projects, systems, processes, or technologies. The process is essential for ensuring that organizations protect the privacy of individuals whose personal data they handle and for complying with data protection laws and regulations.

The steps to implement the PIA process are as follows:

- **Preliminary Assessment**

Identify projects, systems, or processes that involve the collection, processing, or sharing of personal data and may impact individuals' privacy. Consider factors such as data sensitivity and the scale of data processing.

- **Establish the PIA Team**

Assemble a team with expertise in data protection, legal matters, security, compliance, and the specific project or process under evaluation.

- **Data Mapping and Description**

Document the details of the data processing, including the types of data collected, the purposes of processing, data sources, data flows, and data recipients.

- **Privacy Compliance Check**

Examine applicable laws and regulations, such as the GDPR, to ensure compliance. Determine if the processing activity aligns with legal requirements.



- **Risk Assessment**

Analyze the data processing activity to identify potential privacy risks and concerns. Consider factors such as data sensitivity, data access controls, data retention, and the impact on individuals' rights and freedoms.

- **Privacy Impact Identification**

Evaluate how the data processing may affect the privacy of individuals, including the potential for discrimination, harm, or violations of data subjects' rights.

- **Risk Mitigation Measures**

Formulate measures and controls to mitigate identified privacy risks. This may include implementing technical and organizational safeguards, such as encryption, access controls, and anonymization.

- **Documentation**

Document the PIA process, findings, risk mitigation measures, and any consultations conducted. Proper documentation is essential for transparency, accountability, and compliance.

- **Consultation**

If the PIA reveals high privacy risks, engage with relevant stakeholders, data protection authorities, or data subjects to gather input and feedback.

- **Report and Approval**

Summarize the PIA process, findings, and risk mitigation measures in a formal report. Ensure the PIA report is reviewed and approved by relevant stakeholders, data protection officers, legal teams, and management.

- **Integration and Implementation**

Implement the risk mitigation measures and recommendations into the project, system, or process under assessment.

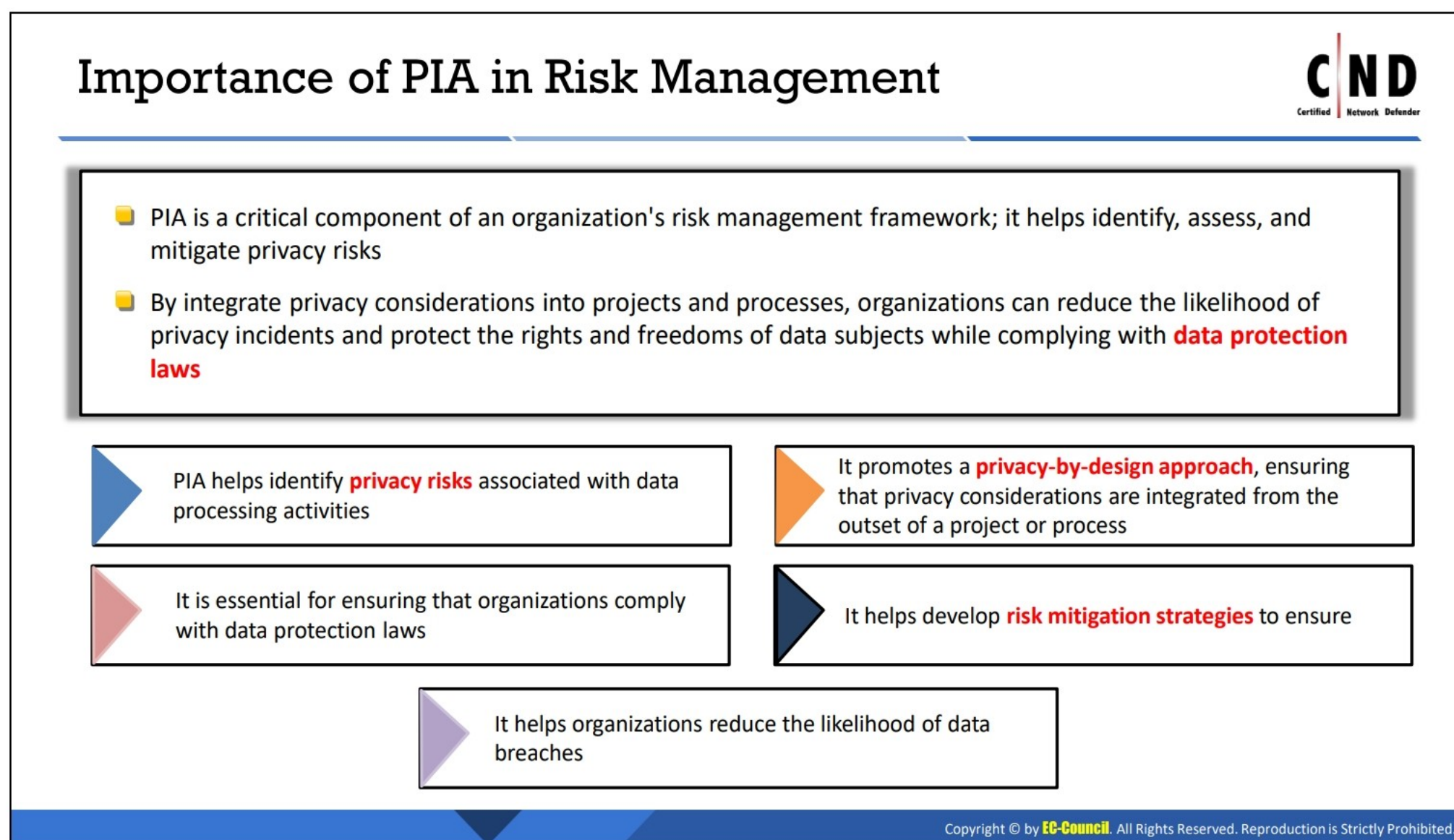
- **Ongoing Monitoring and Review**

Continuously monitor and review the implementation of PIA measures to ensure their effectiveness and relevance.

- **Periodic Review and Update**

The PIA should not be a one-time exercise. Periodic reviews are essential to accommodate changes in data processing activities and evolving privacy requirements.





## Importance of PIA in Risk Management

The systematic identification and analysis of privacy issues by PIA introduces privacy considerations into projects and procedures that assure compliance with data protection regulations, protect the rights of data assets, and reduce the occurrence of privacy incidents, hence improving overall organizational security.

- PIA helps identify privacy risks associated with data processing activities. It assesses and documents key factors about the data processing, and allows responding to privacy risks proactively.
- It is essential to ensure that organizations comply with data protection laws that help organizations reduce the likelihood of data breaches. PIA provides the evidence a compliance standard requires.
- It promotes a privacy-by-design approach, ensuring that privacy considerations are integrated from the outset of a project or process.
- It helps create and implement the required privacy controls and mitigation strategies to address privacy risks, and likelihood of data breaches.



## Privacy Impact Assessment Tools: Mandatly Intelligent Assessment



- Mandatly's intelligent assessment identifies the **case scenarios** in which your need to perform assessments (such as PIA/DPIA)
- It allows conducting privacy assessments to identify and mitigate risk associated with IT systems related to personal data. Risks are **flagged automatically**, providing full visibility to manage your data privacy compliance

The screenshot displays the Mandatly Intelligent Assessment Solution interface. It features a search bar at the top and a table of projects. The 'Assessing the Risks and Impacts' section is highlighted. Below it, a detailed view of an assessment is shown, including a table of data inventory items with their respective risk levels and completion percentages.

Project	Assessment type	Assessment on	Process	Organization
Online Marketing	Privacy by design	System	Digital marketing	Finance
Health monitoring	Privacy Impact Assessment (PIA)	Processing	Monitoring	Quality
Customer info management	Application			

Organization	Process	Domain	Risk	Completion
<b>Assessment: Genesys Data inventory</b>				
Marketing	Digital marketing	Personal data Categories	High	100%
Risk Description: Contains Sensitive data.Categories of special personal data are being processed and consent is not the legal ground for the processing activities				
<b>Assessment: SharePoint Data inventory</b>				
Finance	Vendor Manage / Account payable	Personal data Categories	High	100%
<b>Assessment: Workday Data inventory</b>				
Human Resource	On boarding	Technical Security Measures	High	100%
Human Resource	Talent	Personal data Categories	Low	100%

PIA/DPIA using Mandatly Intelligent Assessment Solution

Source: <https://www.mandatly.com>

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

## Privacy Impact Assessment Tools: Mandatly Intelligent Assessment

Source: <https://mandatly.com>

Mandatly's intelligent assessment identifies the case scenarios in which your need to perform assessments (such as PIA/DPIA) requires. It allows conducting privacy assessments to identify and mitigate risks associated with IT systems related to personal data. Risks are flagged automatically providing the full visibility to manage your data privacy compliance.

### Key Features

- **Assessment portal:** It offers a single source for managing all types of assessments (PIA/DPIA, Vendor, Readiness etc.).
- **Assessment templates:** They allow you to select assessments from standard templates or create your own.
- **Risk assessment:** It automatically assesses the risk and impacts of risk-informed decision-making.
- **Demonstrate compliance:** It allows recording all the activities carried out to ensure transparency and accountability.



<div><div><div></div></div><div>Search...</div></div> <div><div>+ Add</div><div></div></div>				
Project	Assessment type	Assessment on	Process	Organization
Online Marketing	Privacy by design	System	Digital marketing	Finance
Health monitoring	Privacy Impact Assessment (PIA)	Processing Activity	Monitoring	Quality Assurance
Customer info management	Application	System	Sales	Marketing
Project owner: Sandra Lee				
Created on: 07/27/2020 2:59:05 pm				
Last Changed by: Mark Jones				
Last Changed on: 08/02/2020 2:59:05 pm				

Figure 18.4: PIA/DPIA using Mandatly Intelligent Assessment Solution

<div><div><div></div></div><div>Search...</div></div> <div><div>Mitigate</div><div>History</div><div></div></div>				
Organization	Process	Domain	Risk	Completion
Assessment: Genesys Data inventory				
Marketing	Digital marketing	Personal data Categories	High	100%
Risk Description: Contains Sensitive data,Categories of special personal data are being processed and consent is not the legal ground for the processing activities				
Assessment: SharePoint Data inventory				
Finance	Vendor Manage / Account payable	Personal data Categories	High	100%
Assessment: Workday Data inventory				
Human Resourece	On boarding	Technical Security Measures	High	100%
Human Resource	Talent	Personal data Categories	low	100%

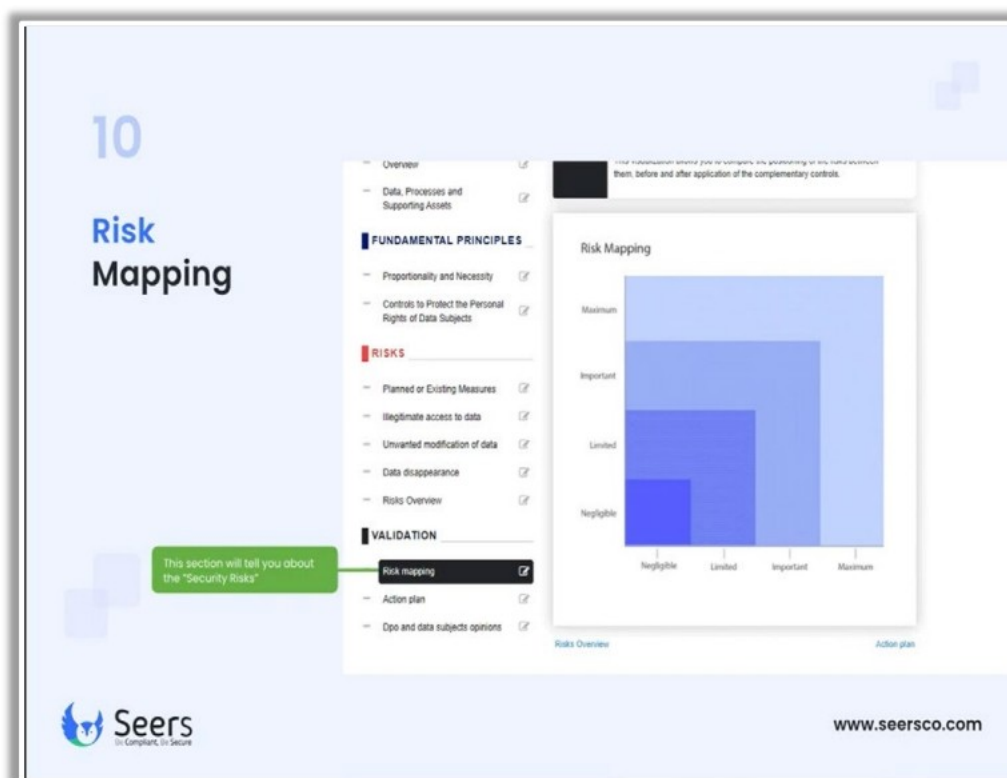
Figure 18.5: Assessing the Risks and Impacts



## Privacy Impact Assessment Tools: Seers



- Seers, a leading provider of PIA solutions, offers a **holistic approach** to identifying and managing privacy risks
- Seers' PIA platform offers a comprehensive privacy risk assessment, enabling organizations to gain deep insights into the privacy risks associated with their **data - processing activities**. This assessment serves as the foundation for building robust privacy safeguards



Risk Mapping using Seers

Source: <https://seersco.com>

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

## Privacy Impact Assessment Tools: Seers

Source: <https://seersco.com>

Seers, a leading provider of PIA solutions, offers a holistic approach to identifying and managing privacy risks. Seers' PIA platform offers a comprehensive privacy risk assessment, enabling organizations to gain deep insights into the privacy risks associated with their data processing activities. This assessment serves as the foundation for building robust privacy safeguards.

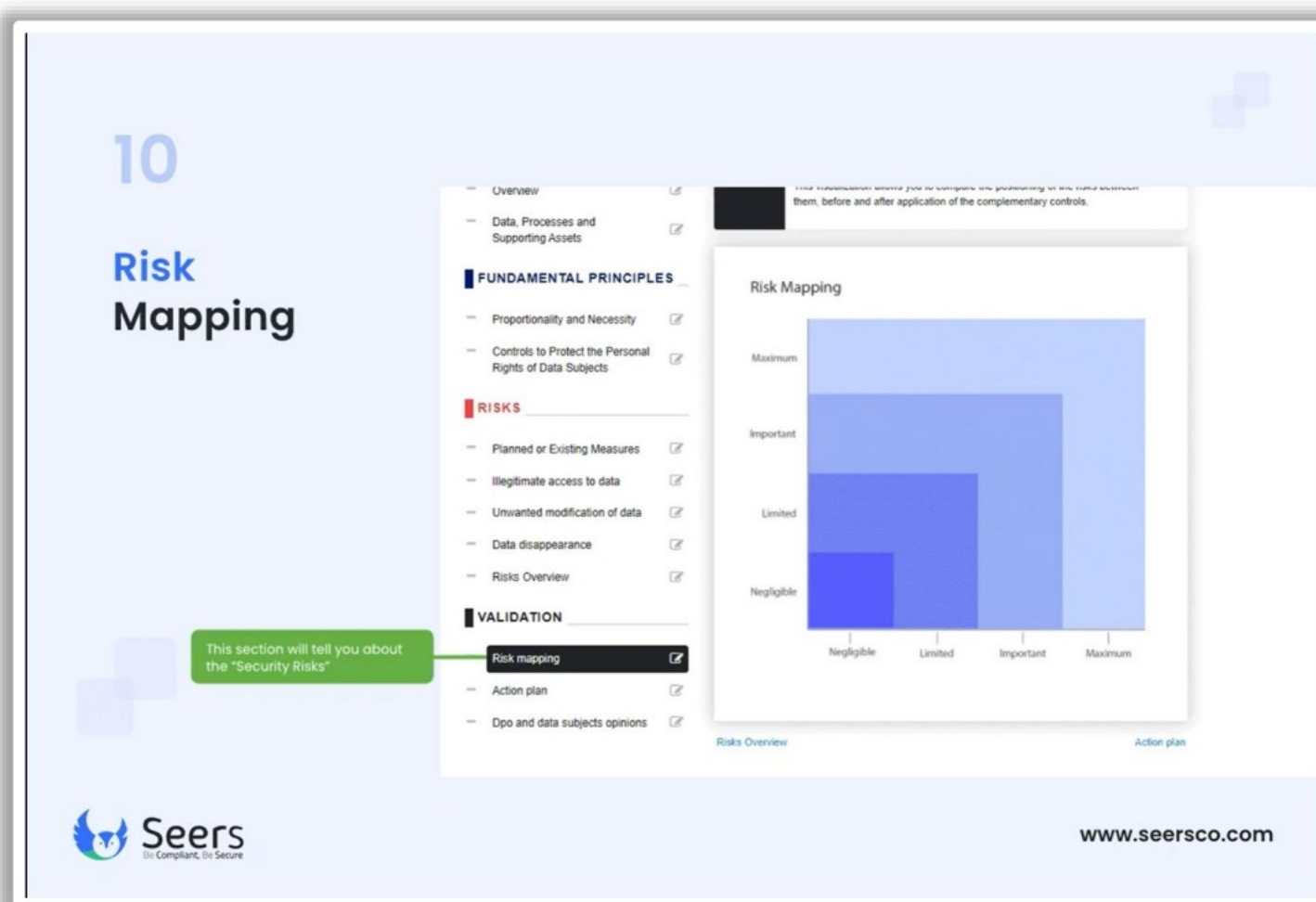












Figure 18.6: Risk Mapping using Seers



## Additional Privacy Impact Assessment Tools



 <b>OneTrust Assessment</b> <a href="https://www.onetrust.com/">https://www.onetrust.com/</a>	 <b>Securiti</b> <a href="https://securiti.ai/">https://securiti.ai/</a>
 <b>TrustArc Assessment Manager</b> <a href="https://trustarc.com/">https://trustarc.com/</a>	 <b>HeyData Data Protection Management</b> <a href="https://heydata.eu/">https://heydata.eu/</a>
 <b>Privado</b> <a href="https://www.privado.ai/">https://www.privado.ai/</a>	 <b>Privacy engine</b> <a href="https://www.privacyengine.io/">https://www.privacyengine.io/</a>
 <b>Smartsheet</b> <a href="https://www.smartsheet.com/">https://www.smartsheet.com/</a>	 <b>Collibra</b> <a href="https://www.collibra.com/">https://www.collibra.com/</a>
 <b>GDPRsimple</b> <a href="https://www.keepgdprsimple.com/">https://www.keepgdprsimple.com/</a>	

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

## Additional Privacy Impact Assessment Tools

Additional privacy impact assessment tools included are as follows.

- **OneTrust Assessment**

OneTrust integrates with existing business processes and tools to simplify the PIA process. Determine and reduce risk with visibility, workflows, and controls to enforce privacy best practices. Demonstrate compliance with real-time regulatory intelligence, insights, and analytics.

- **TrustArc Assessment Manager**

The TrustArc Assessment Manager streamlines processes and records risks for privacy teams. It identifies gaps, records risk, manages tasks and produces compliance reports to meet regulatory requirements. It templates assessments to address PIAs.

- **Privado**

Privado accurately visualizes sensitive data flows across the systems, and sees how data is being collected, used, and shared in real-time. It embeds privacy compliance into the early stages of product design and data lifecycle processes. It ensures privacy commitments are considered before data has been collected, stored, and shared. PIA is directly embedded into development tools.



- **Smartsheet**

Smartsheet is a modern work management platform that brings together people, processes, and technology to empower anyone to drive meaningful change. Organizations of all sizes use Smartsheet to manage projects, automate processes, and gain visibility into programs and portfolios at scale—all on one real-time, centralized platform, accessible from anywhere, on any device.

- **GDPRsimple (DPIA tool)**

GDPR simple is a proprietary tool that can simplify Standard Contractual Clauses (SCC) implementation and demonstration. GDPRsimple provides an implementation of a legal basis to process personal data, individual rights, security assessments, records processing activities, and DPIAs and regulator consultations.

- **Securiti**

Securiti Assessment Automation allows automating records of processing (RoPA) reports and PIAs aligning with global privacy regulations. It allows streamlining privacy-by-design with integrated triggers to dynamically update assessments.

- **HeyData Data Protection Management**

HeyData Data Protection Management platform allows taking advice on data protection issues and any data protection impact assessments.

- **PrivacyEngine (ITS DPIA tool)**

PrivacyEngine ensures processing activities incorporate data protection by design and default from the outset. This tool identifies and addresses privacy risks associated with data processing activities. These assessments are required by data protection regulations. It mitigates risks associated with third-party vendors

- **Collibra**

Collibra assessments help to validate the risks associated with the personal data of data subjects. Collibra helps privacy managers and data protection officers record and track assessments aimed at identifying data usage risks. You can use assessments to identify potential data risks and implement safeguards.



## Privacy Impact Assessment vs Privacy Risk Assessment



Privacy Impact Assessment	Privacy Risk Assessment
A privacy impact assessment is an approach that is helpful in identifying and reducing possible risks to the users', clients', and stakeholders' personal information	A privacy risk assessment acts as a framework that is used to evaluate and examine the risks associated with PII. PIA and DPIA are classified under privacy risk management
It is mandatory to conduct a PIA if a project involves personal information	It is mandatory to conduct this prior to certain tasks before implementing it to eliminate the associated risks
It is conducted by various sub-agencies of the respective countries or through the help of third-party applications tools	It is conducted by the organization's security team. The members of the management board are responsible for identifying and assessing risks in their respective areas of responsibility
It investigates the risks associated with an organization's collection, use, dissemination, and management of personally identifiable information	It provides an early warning system to detect privacy problems and improve the availability of the information internally to avoid costly mistakes in privacy compliance

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

### Privacy Impact Assessment vs Privacy Risk Assessment

Privacy risk assessment works as an early warning system to identify privacy risks. These assessments are conducted and managed internally. By conducting these assessments, the organization could prevent legal implications of non-compliance. Privacy impact assessment comes under the privacy risk assessment. The differences between privacy impact assessment and privacy risk assessment are as follows.

Privacy Impact Assessment	Privacy Risk Assessment
A privacy impact assessment (PIA) is an approach that helps identify and reduce possible risks to the users', clients', and stakeholders' personal information	A privacy risk assessment is a risk management framework that determines the risk of managing PII. It is the parent category of PIA and DPIA
It is mandatory to conduct a PIA if the project involves personal information	It must be conducted before a certain action or task is carried out to eliminate, diminish, or suitably regulate any associated risk
It is conducted by various sub-agencies of the respective countries or with the help of third-party application tools	It is conducted by the organization's security team. The members of the management board are responsible for identifying and assessing risks in their respective areas of responsibility
It is to investigate the risks associated with an organization's collection, use, dissemination, and management of personally identifiable information	It is to provide an early warning system to detect privacy problems and improve the availability of the information internally to avoid costly mistakes in privacy compliance

Table 18.2: Difference Between Privacy Impact Assessment and Privacy Risk Assessment



## Module Summary



- Risk management has a prominent place in the life cycle for securing an organization's network
- Risk management is the process of reducing and maintaining risk at an acceptable level using a well-defined and active security program
- A KRI is a metric showing the risk appetite probability for an organization
- The impact level of a risk depends on the value of assets and resources it affects, and the criticality of the data
- Organizations maintain vulnerability management for their RMFs
- ERM defines the implementation activities specific to how an organization handles risk
- The risk-based vulnerability assessment identifies, classifies, and analyzes vulnerabilities to find a solution to mitigate or remediate them

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

## Module Summary

This module discussed risk management concepts, different RMFs, managing vulnerabilities through vulnerability management programs, and vulnerability assessment and scanning. The following are the key points discussed in this module:

- Risk management has a prominent place in the life cycle for securing an organization's network.
- It is the process of reducing and maintaining risk at an acceptable level using a well-defined and active security program.
- Organizations maintain vulnerability management for their RMFs.
- The risk-based vulnerability assessment identifies, classifies, and analyzes vulnerabilities to find a solution to mitigate or remediate them.