

# **Network Risk and Vulnerability Management**

## **Module 12**



# Network Risk and Vulnerability Management

## Module 12



**Certified Network Defender**

**Module 12: Network Risk and Vulnerability Management**

**Exam 312-38**




The graphic features a dark grey header bar with a yellow square on the left and the 'CND' logo on the right. The logo consists of the letters 'CND' in white, with a vertical yellow line between the 'C' and 'N', and the text 'Certified Network Defender' in small white letters below. The main body of the graphic is a light grey rectangle containing a black rounded rectangle with a yellow border. Inside this black box is a quote in white text. At the bottom of the graphic is a dark grey footer bar with white text.

**CND**  
Certified Network Defender


**“ Risk and vulnerability management is  
a **pro-active** approach of managing  
network security ”**

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




# Module Objectives



- Understanding risk and risk management
- Identifying the key roles and responsibilities in risk management
- Understanding Key Risk Indicators (KRI) in risk management
- Explaining phases involved in risk management
- Understanding enterprise network risk management
- Describing various risk management frameworks
- Discussing best practices for effective implementation of risk management
- Understanding vulnerability management
- Explaining various phases involved in vulnerability management



- Understanding vulnerability assessment and its importance
- Identifying requirements for an effective network vulnerability assessment
- Discussing internal and external vulnerability assessment
- Recalling the steps for effective external vulnerability assessment
- Describing the various phases involved in a vulnerability assessment
- Discussing the selection of an appropriate vulnerability assessment tool
- Discussing the best practices and precautions for deploying a vulnerability assessment tool
- Describing vulnerability reporting, mitigation, remediation and verification



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

This module focuses on network risk and vulnerability management. Organizations are required to manage network risks and vulnerabilities to an acceptable level. This module describes the impact of risk and vulnerabilities on the organization. Dealing with various phases involved in risk and vulnerability management. It will guide you through the various risk levels, roles and responsibilities for the people involved in risk management, different risk management frameworks, vulnerability phases, and the tools used for a vulnerability assessment.

**What is Risk?**

Risk refers to a degree of **uncertainty** or expectation that an adverse event may cause damage to the system

Risk is a function of the following factors:

- Presence of **weakness** in the system (Vulnerability)
- Probability of the occurrence of an adverse event (Threat)
- **Consequences** of the adverse event (Impact)

Potentiality of the risk is best expressed by answering the following questions:

- What is risk?
- What is the impact of risk?
- What is the **frequency** of risk?

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

Risk is an expectation that a threat may succeed to potentially damage resources under specified conditions. In another way, risk can be also defined as:

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

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

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

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

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

Risk is the combination of the following two factors.

- Probability of the occurrence of an adverse event and
- Consequences of the adverse event.


## Impact of Risk

Events which restrict the normal performance and affects the project cost or schedule outcomes. The impact of risk on an organization, process or system is affected by the adverse conditions. The impact indicates the potential seriousness of the risk that occurred.

## Frequency of Risk

Depending on the risk identification and risk assessment, classification of risk depends on the frequency of the occurrence and the severity of their consequences. Frequency and severity are the most important characteristics used to monitor risks. Risks are separated into two categories. Minor risks that don't require further management attention and significant risk that requires management attention and further analysis. The two-dimensional matrix method is a common method to classify risk into three categories, based on the frequency and the severity.

# 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 <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.

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

To analyze risks, you need to work out the frequency or probability of an incident happening (likelihood) and the consequences it would have. This is referred to as the level of risk. Risk can be represented and calculated using the following formula:

**Level of risk = consequence x likelihood.**

There are four risk levels. Those include extremely high, high, medium and low levels. Remember that control measures decrease the level of risk, but do not always eliminate them.

Type of Risk	Consequence	Action
Extreme /High Risk	Serious or Imminent danger	<ul style="list-style-type: none"> <li>Immediate measures should be performed to combat the risk</li> <li>Identify and impose controls to reduce risk to a reasonably low level</li> </ul>
Medium Risk	Moderate danger	<ul style="list-style-type: none"> <li>Immediate action is not required, but it should be implemented at the earliest</li> <li>Implement controls as soon as possible to reduce risk to a reasonably low level</li> </ul>
Low Risk	Negligible danger	<ul style="list-style-type: none"> <li>Take preventive steps to mitigate the risk effect</li> </ul>

TABLE 12.1: Risk Levels

## High Risk Events

These risks warrant specific directed management action to reduce the occurrence of risk and its negative impact. These risks have a high likelihood of occurrence with moderate impact or high impact with the least moderate likelihood. Such risks pose imminent/serious danger and immediate action is necessary. Identify and implement controls to reduce the impact.


## Moderate Risk Events

These risks can either be a high likelihood, low consequence events or low likelihood high consequence events. Individually the high likelihood, low consequence events have very little impact on project cost or the schedule outcomes and will significantly alter the system/organization outcomes. Whereas the low likelihood, high consequence events require periodical monitoring for changes. Recovering from such an impact will require expenditure and additional resources.

## Low Risk Events

Risks categorized as low are usually negligible or can be eliminated from further assessment. During periodical evaluation, users close these low risks or move them to a high risk category. Recovering from such an impact will require minimal expenditures and resources.

# 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%	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%	High Probability	Low	Medium	High	High	Extreme
41 - 60%	Equal Probability	Low	Medium	Medium	High	High
21 - 40%	Low Probability	Low	Low	Medium	Medium	High
1 - 20%	Very Low Probability	Low	Low	Medium	Medium	High

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

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

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

TABLE 12.2: Risk Determination Matrix

The above figure is the graphical representation of the risk matrix which is displayed for visualizing the risk and comparing risks. It is the simple way for analyzing risks and differentiates the two levels of risk.

- Likelihood/The chance of risk occurring
- Consequence/Severity of the risk event that occurred


Each cell in the risk matrix represents the combination of likelihood and severity. The seriousness of the risk is related to the likelihood and the impact. Depending on the occurrence, the risk likelihood has five categories including:

1. **Very High Probability:** The probability of occurrence is more than 80% and will most likely cause more problems.
2. **High Probability:** The probability of occurrence is 61-80% and will likely cause more problems.
3. **Equal Probability:** The probability of occurrence is 50/50.
4. **Low Probability:** The probability of occurrence is low about 21-40%, this occurrence should not be ruled out. These occurrences are still a risk.
5. **Very Low Probability:** The probability of occurrence is rare and exceptional, which have less than a 20% chance to occur.

Depending on the severity, the risk consequences are included in five categories including:

1. **Insignificant:** These risks cause a negligible amount of damage.
2. **Minor:** These risks cause damage, but not to a large extent and do not affect the network significantly.
3. **Moderate:** These risks do not impose a great threat, can inflict sizable damage.
4. **Major:** These risks have significantly large consequences, which lead to a great loss to the organization.
5. **Severe:** These risks make the network completely unresponsive and are the top priority risk for 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 is the process of identifying, assessing, response and implementing the activities which control how the organization manages the potential effects. Risk management has a prominent place throughout the security life cycle. Risk management is a continuous and ever-increasing complex process. The type of risks vary from organization to organization, preparing a risk management plan will be common between all organizations.


## Risk Management Objectives

- The main objective of risk management is to identify the potential risks.
- Identify the impact of risks and help the 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 effect.
- Create awareness among the security staff, develop strategies and plans for risk management strategies that last.

## Risk Management Benefits

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

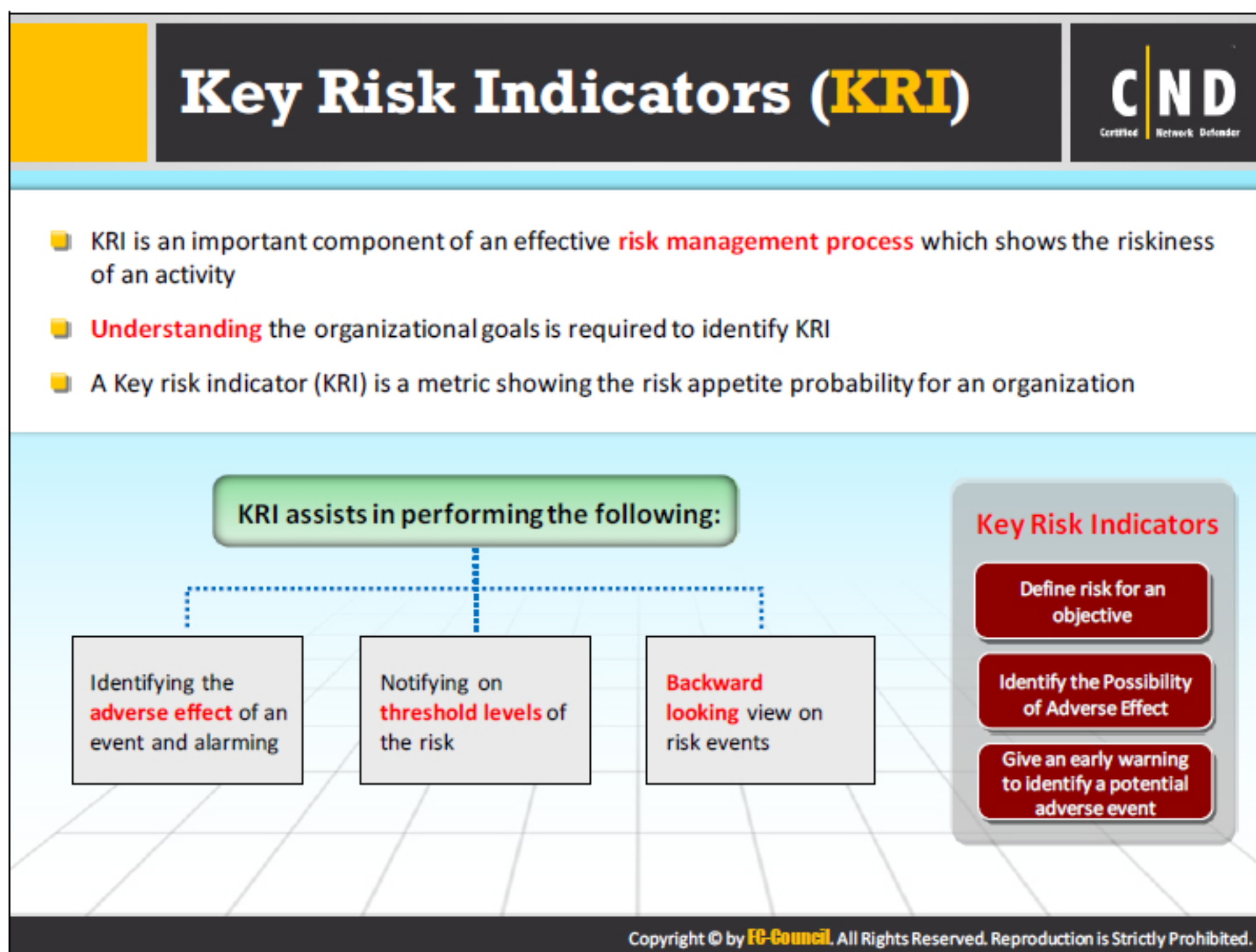
- Focuses on the potential risk impact areas.
- Risks can be addressed according to a level.
- Improves the risk handling process.
- Allows security officers to act effectively in adverse situations.
- Enables effective use of resources.

<h1>Key Roles and Responsibilities in Risk management</h1>		
	<b>Senior Management:</b> The support and involvement 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 trade-off 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 security controls	
	<b>Security Awareness Trainers :</b> Responsible for developing and providing appropriate training on the risk management process	
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.		

Risk management team member roles and responsibilities are:

- **Senior Management:** It is the responsibility of the senior management to supervise the risk management plans carried out in an organization. They develop policies and techniques required to handle the commonly occurring risks. Senior managers, through their expertise can design the steps required for handling future risk.
- **Chief Information Officer (CIO):** The person entitled with the position “Chief Information Officer” is responsible for executing the policies and plans required for supporting the information technology and computer systems of an organization. They play a vital role in the formation of basic plans and policies for risk management. The main responsibility for a CIO is to train employees and other executive management regarding the possible risks in IT and its effect on business.
- **System and Information Owners:** System and information owners mainly monitor the plans and policies developed for information systems. Their responsibilities include:
  - Take part in all discussions regarding the configuration management process.
  - Keep a record of the information system's components.
  - Conduct an investigation on all the changes in the information systems and its 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 the system.
- **Business and Functional Managers:** They are responsible for maintaining all management processes in an organization. They are empowered with an authority to manage almost all the 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 (ISSO):** ISSO provides required support to the information system owners with the selection of the security controls for protecting the system. They also play an important role in the selection and the amendment of the security controls in an organization.
- **IT Security Practitioners:** The IT security practitioners protect the personnel, physical and information security in an organization. The main responsibilities include:
  - Framing better security methods in the organization.
  - Developing methods that fulfil 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.
  - Supervise the overall security measures taken in an organization.
- **Security Awareness Trainers:** Security awareness trainers provide IT security awareness and training programs in an organization. People responsible for this role will be subject matter experts and validate only proper content is included in the program.



Key Risk Indicators (KRIs) are an important component of an effective risk management process, which show the riskiness of an activity at an early stage. Understanding of the organizational goals is required to properly identify KRI. It is a metric which is capable in showing the risk appetite probability of the organization. KRIs are the most important indicators of an organization's overall health helping reduce loss and prevents risk exposure. Risk exposure is prevented by measuring the risk profiles and risk situations in advance, before the risk event occurs.

KRI assists in performing the following:

- Event effect identification
- Threshold level notifications
- Backward looking view on risk events

The KRI should accurately measure and reflect the negative impact on the organization's key performance indicators (KPI). KPI is the metrics that assess the progress of an organization reaching its goals. Providing leading indicator information about emerging risks from external events that affect the demand for an organization's products or services. The KRI represents key ratios, the organization tracks as indicators of evolving risks and potential opportunities, which show the necessary actions. The KRI framework is managed by the KRI manager with the help of the KRI libraries. KRIs can link to multiple risks and controls, while the user notes the KRI values manually through an intuitive wizard and uploads additional KRI values from

spreadsheets, using the powerful Force.com data loader or input automatically via the Force.com web services API.

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



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

The 4 key steps commonly termed as risk management phases are:

1. Risk Identification
2. Risk Assessment
3. Risk Treatment
4. Risk Monitoring & Review

Every organization should follow the above steps while performing the risk management process. The initial step in this process is to identify the risk events before they cause harm/damage. After identifying and assessing the severity of the risk event across an organization, the employees need to take certain actions to control the risk situation and reduce the damages inflicted from it. The last and important step is to monitor and review, to ensure that the controls are working and there is no danger for new risks.

## Risk Identification

It is the initial step of the risk management plan. The main aim is to identify the risks before they cause harm to the organization. The risk identification process depends on the skill set of the people and it differs from one organization to another organization. It identifies the sources, causes, consequences, etc. of the internal and external risks affecting the security of the organization. Risks commonly originate from five key areas.

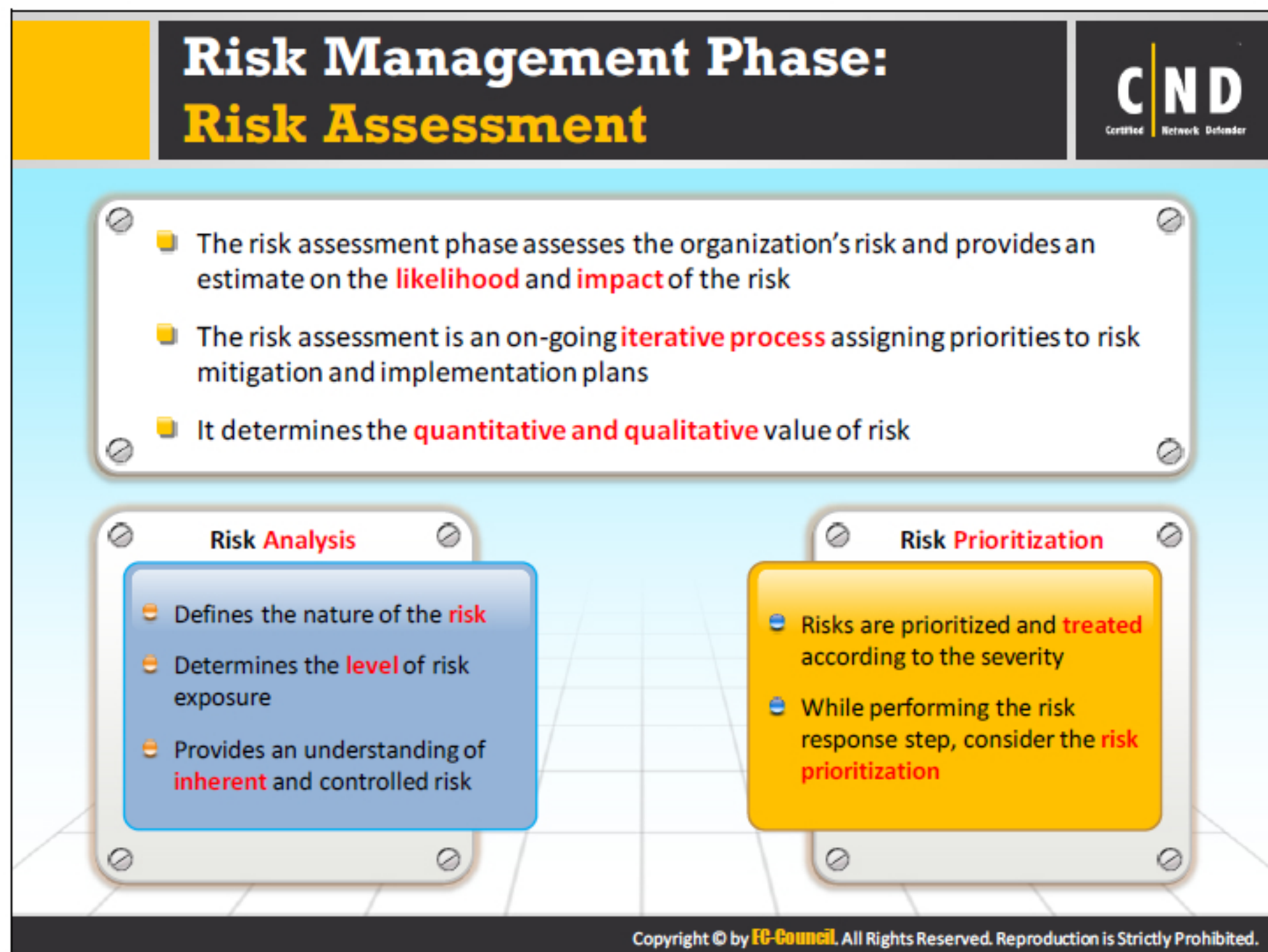
The purpose of risk identification is to generate a list of threats and opportunities based on those events that may enhance and prevent the achievement of objectives. They are:

- **Environment:** Risks associated with the environment can include tight work spaces, clutter, hot/cold environments, smoking, poor lighting, and electrical hazards.
- **Equipment:** Risks associated with equipment are poor repair condition, not working, unavailable, and inappropriate for the task.
- **Client:** Risks happen with clients due to conditions changing, unpredictable movements, and poor communication.
- **Tasks:** These include insufficient time allocated, repetitive tasks, work design, task organization, maintaining a fixed posture, poor postures, and insufficient employee numbers.

## Steps in Risk Identification

- **Establishing Context:** The employee defines the external and internal environment and understands the current conditions in which the organization operates.
- **Quantifying Risks:** Determines the effect of risk and calibrates the possible outcome of the risks.

Risk identification reduces the bias in the risk assessment while at the same time reduces any for likelihood or impact in the future. There are many ways to identify risks, there are documents and tools available to support the risk identification process. Most identification processes begin with an issue examination and concerns created by the development team. The risk identification process varies, depending on a few factors such as the nature of the network and the risk management skills of the team members.



The risk assessment phase assesses the organization's risks and estimates the likelihood and impact of those risks. Risk assessment is an ongoing iterative process and assigning priorities for risk mitigation and implementation plans. This 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.

The risk assessment determines the kind of risks present, the likelihood and severity of risk, priorities and plans for risk control. Organizations perform a risk assessment when they identify a hazard, but are not able to control it immediately. After performing a risk assessment, you need to update all information facilities at regular intervals.

After assessing the risks, prioritize them depending on their severity or impact on the organization. The prioritized list helps develop and handle the plans, preparing a handling task sequence list, and allocating handling resources. The numbers represent risk prioritization in accordance with their severity such as:

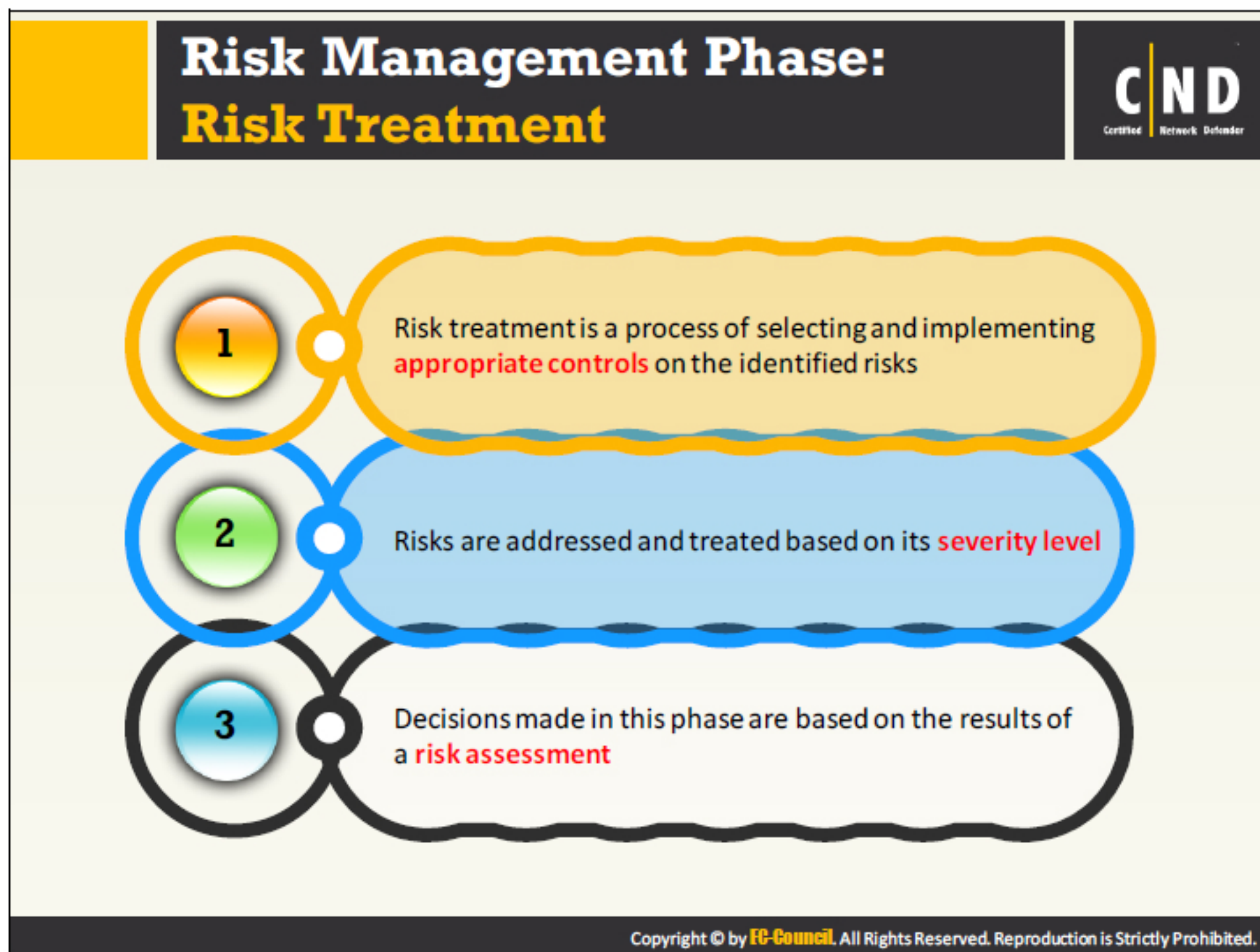
**1-2:** The risks with a priority of 1-2 need to be eliminated immediately (usually within 24 hours) or if you cannot eliminate it, reduce the risk of the hazard to a lower rating by implementing at least one control measure.

**3-4:** Risks with this priority need to be eliminated or control the hazard 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:** Defines the nature of the risk and determines the level of risk exposure. It provides an understanding of the inherent and controlled risk.
- **Risk Prioritization:** Risk prioritization is the process of rating a risk during its analysis according to its severity and designing a response plan.



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

- Select the appropriate method of treatment
- People responsible for treatment
- Costs involved
- Benefits of treatment
- Likelihood of success
- Ways to measure and assess the treatment

Once you have decided how to treat identified risks you need to develop and regularly review the risk management plan. The different options that are performed to treat the risks are avoiding the risk itself (avoiding the activities that lead to a rise of risk), reducing the risk (reducing the likelihood of the risk occurring and reducing the impact if the risk occurs), transfer the risk (shift the risk responsibilities to another party through insurance or partnership).

Accept the risk (if it cannot be avoided or transferred). Employees will perform the following actions to minimize or to eliminate the 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.

<div> <div></div> <div> <b>Risk Management Phase:</b>  <b>Risk Treatment Steps</b> </div> <div>CND Certified Network Defender</div> </div>	
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 <b>mitigation</b> has exceeded the impact of the risk on the network
Risk Avoidance	<b>Eliminating</b> the cause and consequences of risk
Risk Planning	<b>Managing</b> the risk by a risk mitigation plan which <b>prioritizes</b> the risks, <b>implements</b> and <b>maintains</b> the controls for the risks throughout the risk management lifecycle
Research and Acknowledgment	Vulnerability research and finding the controls to <b>rectify</b> them
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.	

A risk treatment can change the likelihood for occurrences of risk by considering the options and detailed designs required to select the appropriate risk treatment step. Risk treatment involves a series of options for mitigating the risks, assessing the options and preparing and implementing the action plans. The risk with the highest rate is dealt with first. The options available according to the type and nature of the risks are:

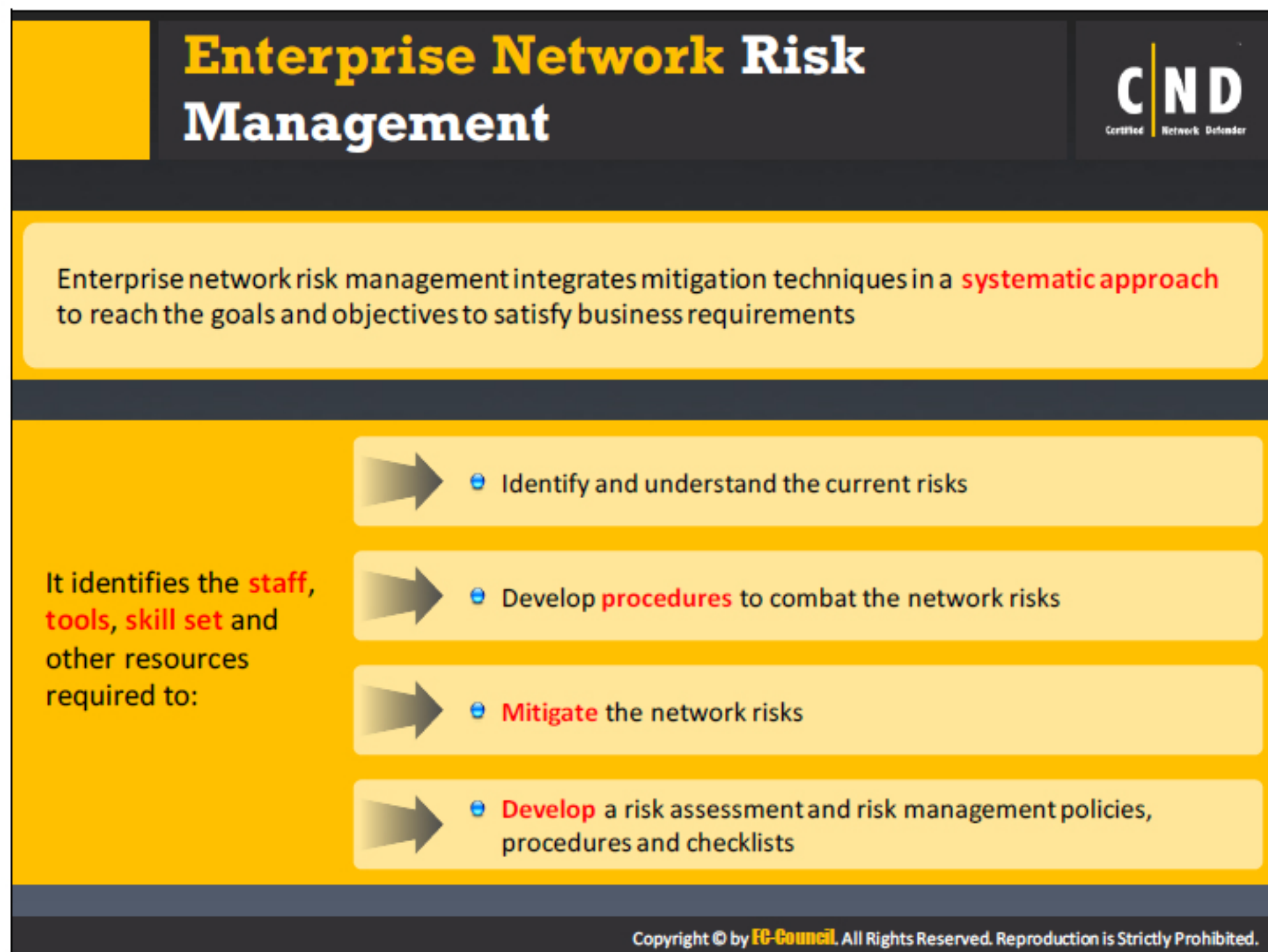
- **Avoid:** Avoiding the factor that enhances the risk factor of any process in the business or finding an alternative that goes well with business needs.
- **Reduce:** Finding ways to reduce the likelihood rate of risk to an acceptable level.
- **Share or Transfer:** Transferring the risk factor to a third party, so they manage the risk levels.
- **Accept:** The risk factor should be at an acceptable level.

The steps taken in risk treatment differ from case to case. Stakeholders and process owners mutually decide these steps. Key points while considering risk treatments are:

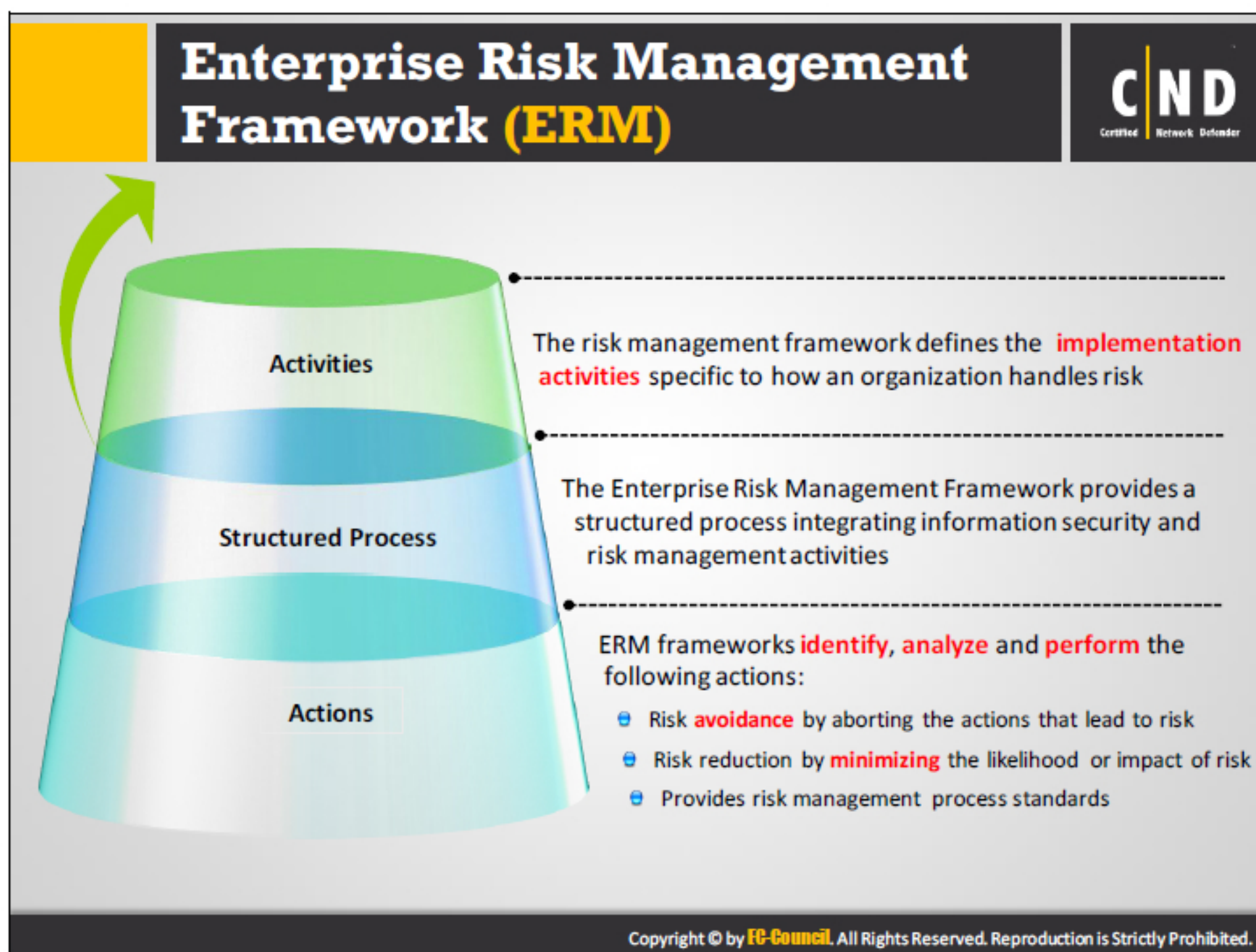
- Implement an appropriate risk treatment option.
- Adequate resources are available while implementing the risk treatment plan.
- The risk treatment plan should reduce the risk factor to a certain acceptable level.
- If there are risks to be handled immediately, remedial actions are taken for those risks.



An effective risk management plan requires a tracking and review structure to ensure effective identification and assessment of the risks as well as the use of appropriate controls and responses. Perform regular inspections of policies and standards, as well as review them regularly to identify the opportunities for improvement. The monitoring process assures there are appropriate controls in place for the organization's activities and that the procedures are understood and followed. The tracking and review process should determine the measures adopted, the procedures adopted, and information gathered for undertaking the assessment was appropriate.



According to the Enterprise Risk Management Framework (ERM), a risk is the possible event that can have a negative impact on an enterprise. The impact will be on any of the following: the resources of the enterprise, i.e. Human and revenue, facilities by the enterprise, its clients, and market value. Financial organizations describe ERM as a combination of risks based on credit, interest, liquidity, market, and operational.



ERM provides a framework for risk management, which typically involves identifying events that are relevant to the organization's objectives. The ERM framework provides an organized process combining information security and risk management events.

ERM frameworks identify, analyze and perform the following actions:

- Risk avoidance by aborting the actions that lead to the risk.
- Reduction of risk by reducing the likelihood or impact of the risk.
- Standardizes the risk management process.

ERM is the risk based approach to manage an enterprise. ERM involves addressing the needs of various stakeholders who want to know about the broad spectrum of risks faced by the organization to ensure they can easily and appropriately manage. The key activities involved in managing enterprise-level risk i.e., the risk resulting from the operation of an information system are:

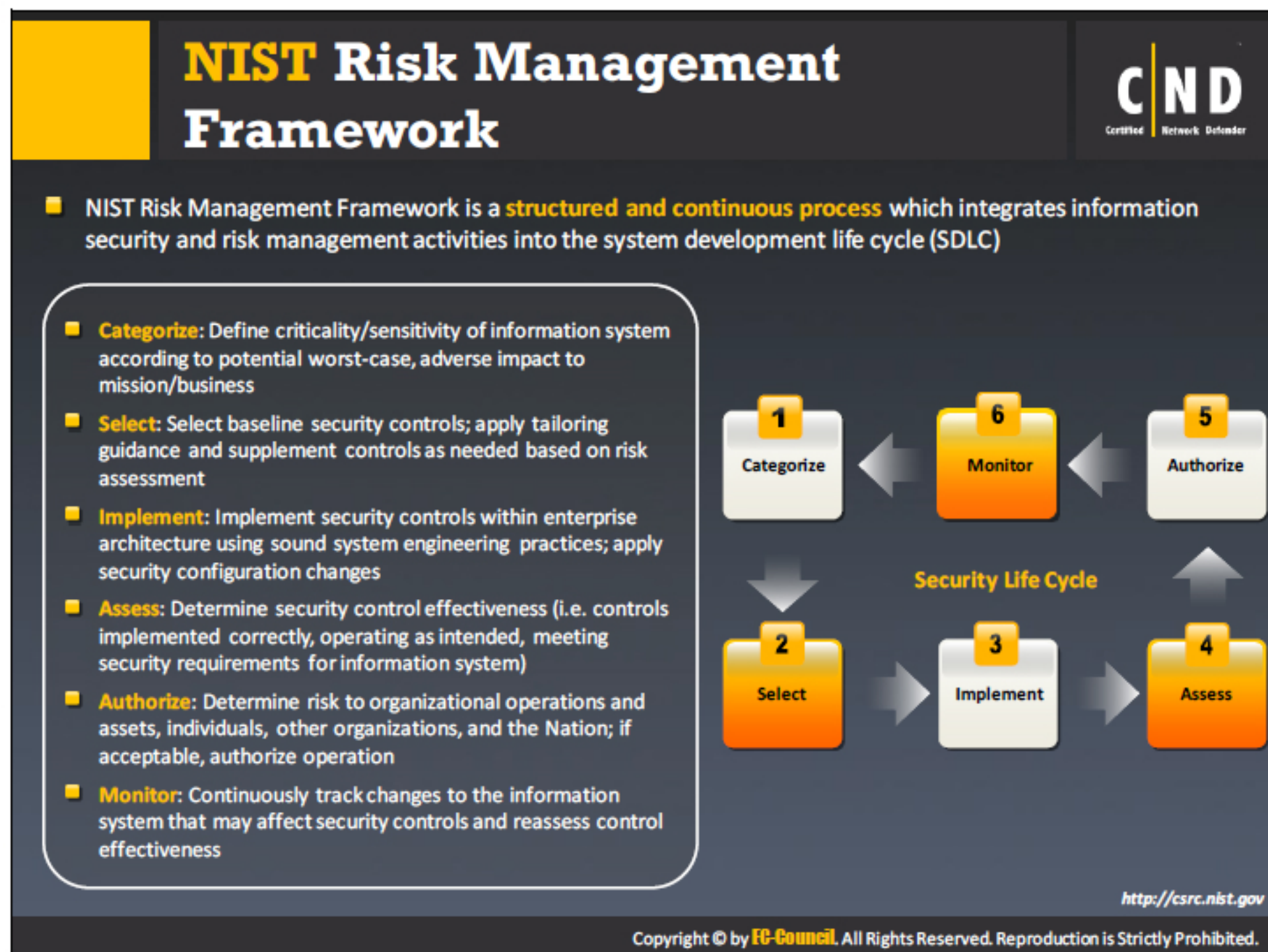
- Classification of the information system.
- Selection of appropriate security controls.
- Refine the selected security control set based on the risk assessment.
- Maintain the document for all selected security controls in the system security plan.
- Implementation of the security controls.

- Security controls assessment.
- Determining agency-level risk and risk acceptability.
- Authorizing information system operation.
- Monitoring security controls on a continuous basis.



Organizations manage risks and have a number of departments or risk functions that help in identifying and managing risks. A common goal or the challenge of ERM is improving the capability and coordination, while integrating the output to provide a unified picture of risk for stakeholders and improving the organization's ability to manage the risks effectively. The Enterprise Risk Management Framework has the following additional goals:

- Convey the organization's policies, approach and attitude towards risk management.
- Ensure that organization should meet risk reporting commitments.



NIST Risk Management Framework is a structured and continuous process which integrates information security and risk management activities into the system development life cycle (SDLC). The NIST risk management framework follows a security life cycle, which involves six stages. The framework's six stages are:

- **Categorization of Information System:**

This is the initial stage of the NIST risk management framework which involves defining criticality or sensitivity of the information system according to the potential worst-case. This shows the adverse impact to mission or business.

- **Selection of Security Controls:**

Initially categorize the information system, and then select the baseline security controls under a NIST Risk Management Framework. Apply tailoring guidance and supplement controls if needed based on risk assessment.

- **Implement Security Controls:**

Implement security controls within the enterprise architecture using sound system engineering practices. Apply security configuration settings.

- **Assess Security Controls:**

Determine security control effectiveness that is the controls implemented correctly and effectively, operating as intended, and meeting security requirements for information system.

- **Authorize Information System:**

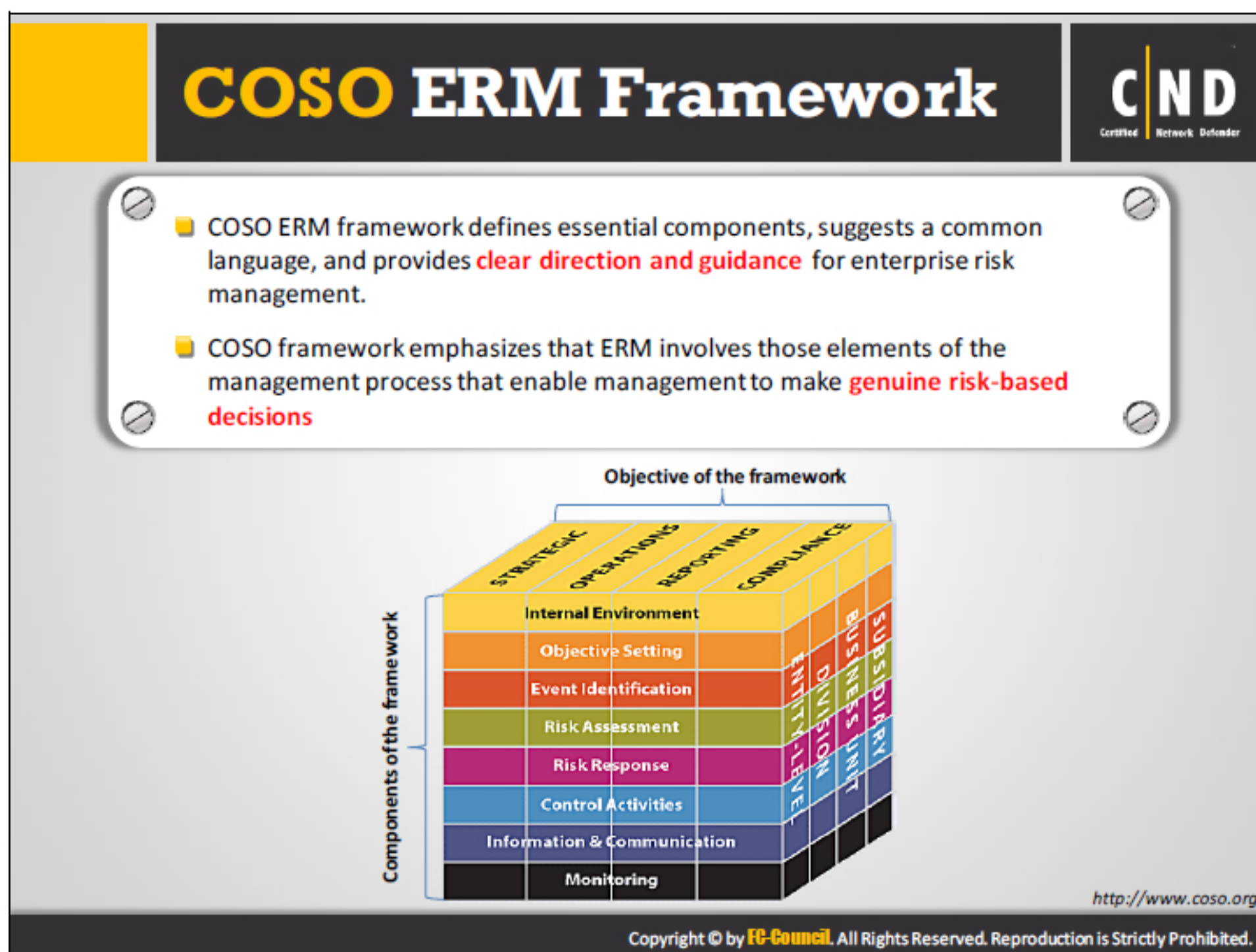
Determine risk to organizational operations and assets, individuals, other organizations, and the nation if acceptable, authorize the operation.

- **Monitor Security State:**

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

---

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



COSO ERM framework defines enterprise risk management as a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise. It is designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of the entity's objectives. The framework defines essential components, suggests a common language, and provides clear direction and guidance for enterprise risk management.

COSO framework emphasizes that ERM involves those elements of the management process that enable management to make genuine risk-based decisions.

### Objectives of the COSO Framework

The framework has four objective categories, which portray the ability to completely focus on enterprise risk management. The categories include

- Strategic objectives of an ERM are high level and aligned with an entity's mission.
- Operation objectives refer to the effective and efficient use of resources.
- Reporting objectives surround an entity's need for reliable reporting.
- Compliance objectives align with an entity's need to comply with applicable laws and regulations.

The categorization of entity objectives allows a focus on separate aspects of enterprise risk management. The categories overlap and a particular objective can fall into more than one category as well as address different entity needs and may be the direct responsibility of different executives.

## Components of Enterprise Risk Management Framework

Enterprise risk management consists of eight interrelated components, which arise from the way management runs an enterprise and are involved in the management process.

The components of ERM are:

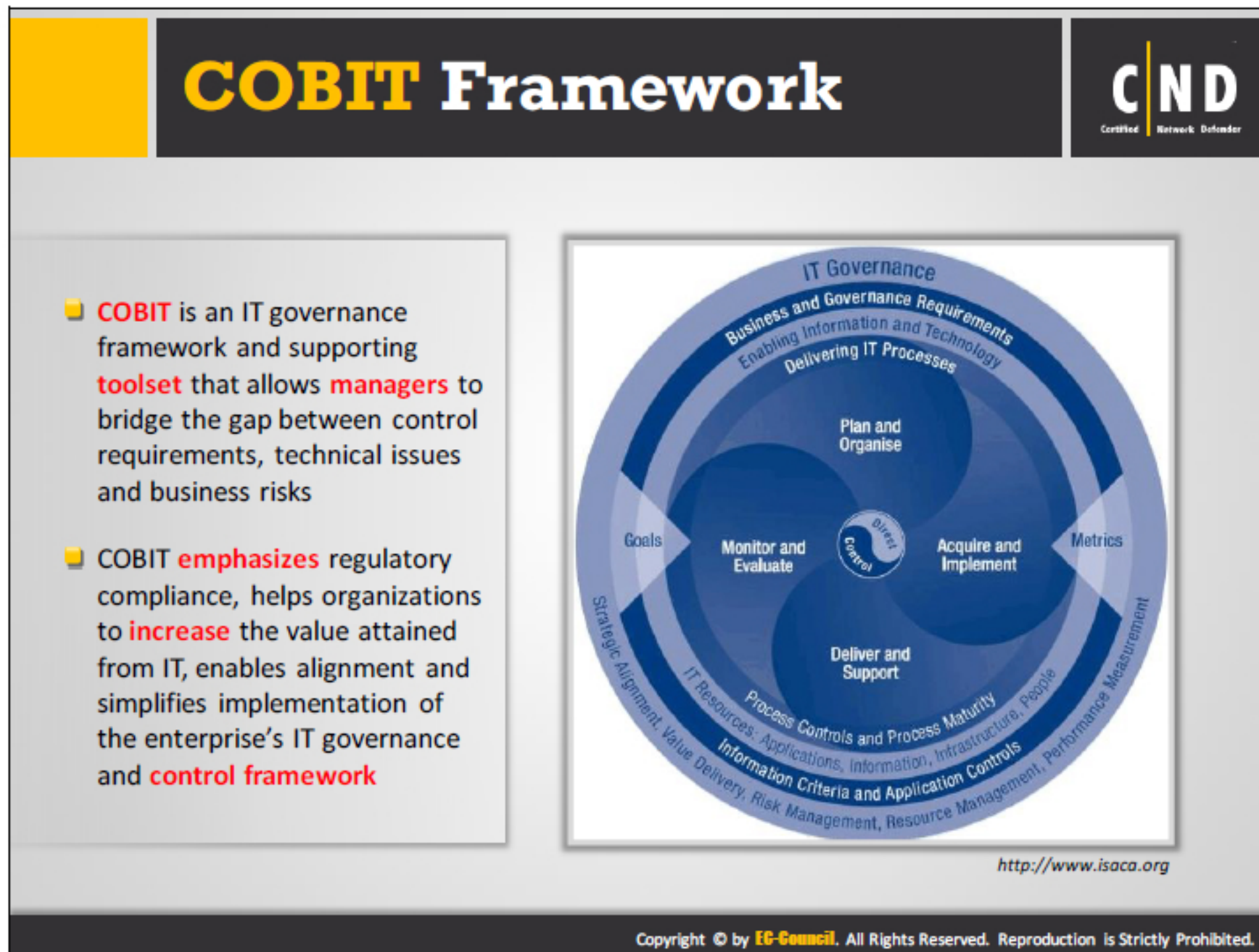
- **Internal Environment:** It contains the tone of an organization and sets the basis for the processes such as viewing and addressing by an organization. This includes the risk management philosophy and risk appetite, integrity and ethical values and the environment in which they operate.
- **Objective Setting:** A framework should define objectives before management can identify potential events affecting them. Enterprise risk management ensures that management has in place a process to set the objectives that support and align with the organization's mission and are consistent with its risk appetite.
- **Event Identification:** The organization should identify the internal and external events affecting their completion of objectives and differentiate the risks from opportunities. The channel supports the opportunities to the management strategy or objective-setting processes.
- **Risk Assessment:** Risk assessments include analyzing the risks by considering their probability and impact as a basis for determining the process to manage them. Risk assessments should be on an inherent and a residual basis.
- **Risk Response:** Management selects the risk responses avoiding, accepting, reducing, or sharing risk by developing a set of actions to align risks with their risk tolerance and risk appetite.
- **Control Activities:** Every organization has policies and procedures which are established and implemented to ensure an effective execution of the risk responses.
- **Information and Communication:** Enterprises should identify, capture, and communicate relevant information in a detailed process and timeframe that can allow people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the organization.
- **Monitoring:** The organization should monitor their risk management process and modify them if necessary. Enterprises can complete monitoring through on-going management activity, separate evaluations, or both.

## Relationship between Objectives and Components:

There is a direct relationship between objectives, which are the organization's goals and the enterprise risk management components, which are the important features needed to achieve those goals. Components are criteria for effective enterprise risk management that function properly if there are no material weaknesses and if the organization succeeds in bringing down the risks within its appetite.

---

Source: [www.ciso.org](http://www.ciso.org)



COBIT is a business framework for IT governance and management toolset enabling managers to bridge the gap between control requirements, technical issues and business risks. The framework offers globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems.

COBIT emphasizes regulatory compliance, helping organizations increase the value attained from IT, enables alignment and simplifies the implementation of the enterprise's IT governance and control framework.

COBIT helps enterprises of all sizes to:

- 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.
- Support compliance with relevant laws, regulations, contractual agreements and policies.

The COBIT Framework is based on five key principles for the governance and management of enterprise IT that include:

- Meeting Stakeholder Needs
- Covering the Enterprise End-to- End
- Applying a Single, Integrated Framework
- Enabling a Holistic Approach
- Separating Governance from Management

---

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

## Risk Management Information Systems (RMIS)

**CND**  
Certified Network Defender

- RMIS is a management information system allowing the storage, management, analysis and the ability to retrieve the **risk information** for an organization's network
- Organization's incorporate the **risk management framework** with the RMIS to optimize the risk management process

**Network security professionals use RMIS to:**

- Assess the risk and its adversary
- Generating different types of reports
- Target specific risk factors
- Data can be efficiently managed and analyzed with limited resources

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

RMIS is a medium which stores, manages, analyzes, and retrieves the risk information of an organization network from a single system. The system assists in consolidating property values, claims, policy, and exposure information to enable the user to monitor and control the overall cost of risk. RMIS not only provides a means to examine the organization's network but also addresses the risks.

The organization needs to incorporate the risk management framework with the RMIS to get optimum results as these systems act as risk management instruments in the organization. Network security professionals use RMIS to do the following:

- Assess the risk and its adversary.
- Generating different types of reports.
- Target specific risk factors.
- Data can be efficiently managed and analysed with limited resources.

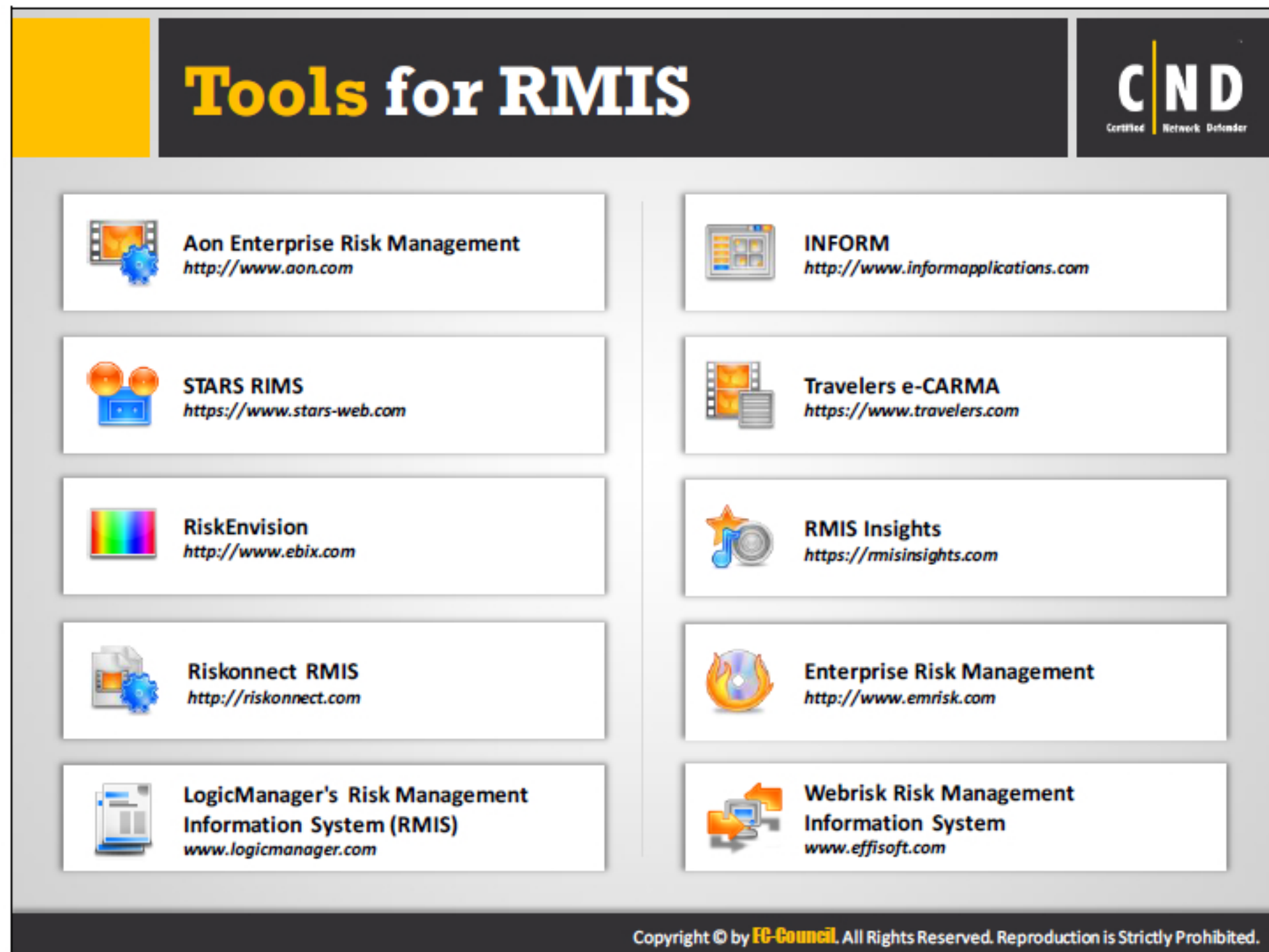
The main objective of RMIS is to combine information and store it in one place. This assists risk managers in making many critical decisions. The three main advantages of RMIS are:

- Better dependability of data as it reduces data redundancy and data errors.
- Helps reduce the cost factor in an organization due to better risk management through RMIS.

- RMIS in compliance with the company standards, helps them to implement risk management policies resourcefully.

RMIS generates reports on various aspects and these reports enable the organization to have a consolidated view of the network risks and manage them. Types of RMIS reports generated are dependent on the type of request sent. The RMIS generates the following types of reports:

- **Standard Reports:** RMIS generates standard reports as a response to common queries. These reports do not contain categorical data.
- **Ad-hoc Reports:** The system also generates the ad hoc reports as a response to special queries. They contain categorical data.



### Aon Enterprise Risk Management

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

Enterprise Risk Management (ERM) provides a framework to understand and respond to business uncertainties and opportunities with relevant risk insight delivered through common, integrated risk identification, analysis and management disciplines. ERM enhances organizational resiliency by improving decision making, strengthening governance and supporting a risk intelligent culture.

### STARS RMIS

Source: <https://www.stars-web.com>

STARS RMIS supports comprehensive risk management, enterprise risk management (ERM), claims management, compliance and safety management and peer benchmarking.

### RiskEnvision

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

RiskEnvision offers a web-based total risk management and claim administration solution. RiskEnvision supports risk management and claims administration functions including payment processing, reserve management, form letters and correspondence, policy management, diary, reporting, and more for Auto, GL, Product, Property, and Worker Compensation lines of insurance coverage in a user-friendly application, with minimal maintenance overhead.

## **Riskconnect RMIS**

Source: <http://riskconnect.com>

A risk management software platform, which enables customers and risk professionals to automate their entire risk management process. It is an approach towards claims, litigation, exposure, policy management and more with technology.

## **LogicManager's Risk Management Information System (RMIS)**

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

LogicManager's Risk Management Information System accomplishes policies and reduces claims and track litigation with risk management techniques.

## **INFORM**

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

INFORM provides a set of reporting tools and data intake tools for both basic and complex needs. The reporting tool provides the platform of BI Intelligence based reporting solution from very basic to very complex needs.

## **Travelers e-CARMA**

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

Travelers e-CARMA is a risk management information system that helps users to manage loss costs. The main activities of Travelers e-CARMA include:

- Analyses data loss
- Keep up with claim activity
- Discover loss trends

## **RMIS INSIGHT**

Source: <https://rmisinsights.com>

RMIS INSIGHT simplifies sharing, comparing, and acting on RMIS data analytics. It supports both Claim and Policy Analytics.

## **Enterprise Risk Management**

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

Enterprise Risk Management provides business key support and guidance in computer security risk assessment and the management of technology risk.

Enterprise Risk management helps:

- Identify potential risks
- Evaluate them
- Provide recommendations to mitigate the identified risks


## **Webrisk Risk Management Information System**

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

Webrisk RMIS helps risk managers manage their daily operations easier, and achieve sustainable results. Features of Webrisk RMIS include:

- Business unit management
- Risk Mapping by axes of analysis
- Asset evaluation for renewals and on-line renewal data gathering
- Property and fleet management
- Geolocation of sites and risks
- Prevention management
- Policy program management
- Incident and claim management and notification
- Sophisticated ad hoc reporting

## 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	Accomplishes the strategic and operational goals of the organization
Provide a consistent risk management framework	Combat the existing and emerging risks	Facilitates with assistance in taking strategic management decisions
Provide the overall direction and purpose of performing risk management	Integrate operational risks into the risk management process	Meets legal and regulatory requirements

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

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

The policy will develop and establish essential procedures and processes to address and minimize information security risks. The policy will protect the Confidentiality, Integrity, and the Availability of a company's IT assets. The Enterprise network risk management policy addresses information security issues and their impact. It also suggests measures to keep them secure from both internal and external risks.

The risk management policy also outlines different aspects of risk and identifies people to manage the risk in the organization. Risk management is the process of balancing operational and economic costs for protective measures while achieving the objectives and business goals. The policy should have characteristics including dynamic, real and applicable, built to achieve long term organizational goals, and is easy to maintain.

The risk management security policy addresses the following issues related to the security of an organization:

- Internal controls
- Risk acceptance policy
- Risk Assessment

- Risk Mapping
- Contingency Planning
- Incident Response
- Business asset valuation
- Mission Impact Assessment
- Audit and assessment policy
- Disaster recovery/business continuity policy
- Key indicators to monitor the effectiveness of control

Organizations should consider certain objectives while developing a new risk management policy that are in line with their work and also help earn profits. The purpose of a risk management policy is to offer better risk management through identification, management, and acceptance across all segments of an organization. Some of the most common objectives are:

- Should meet legal and regulatory requirements.
- Assists strategic management decisions.
- Accomplish organizational strategic/operational goals.
- Integrate operational risks in to risk management.
- Combat existing and emerging risks.
- Manage the risks with adequate risk mitigation techniques.
- Provide the overall direction and purpose for performing risk management.
- Provide a consistent risk management framework.
- Equip the organization with the required skills to identify and treat risks.

	<b>Best Practices for Effective Implementation of Risk Management</b>	<b>CND</b> Certified Network Defender
✓	Track and <b>monitor</b> internal and external risks of the organization at <b>regular intervals</b>	
✓	<b>Establish</b> a risk management <b>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 <b>planning</b> process	
✓	Identify the potential risks to the <b>network</b>	
✓	Prioritize the risks based on its <b>impact on the enterprise network</b>	
✓	Specify the responsibilities for risk managers with their respective <b>domains</b>	
✓	Regularly <b>review</b> and <b>update</b> the risk management policy	
Copyright © by <b>EC-Council</b> . All Rights Reserved. Reproduction is Strictly Prohibited.		

Effective risk management depends on the implementation of predefined or planned proposals. Therefore, it is crucial to consider some best practices for implementing the plan:

- Enlist various improvement options.
- Identify the threats and risks arising from user errors and analyze the risks caused in normal and fault conditions.
- Always make sure the 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.

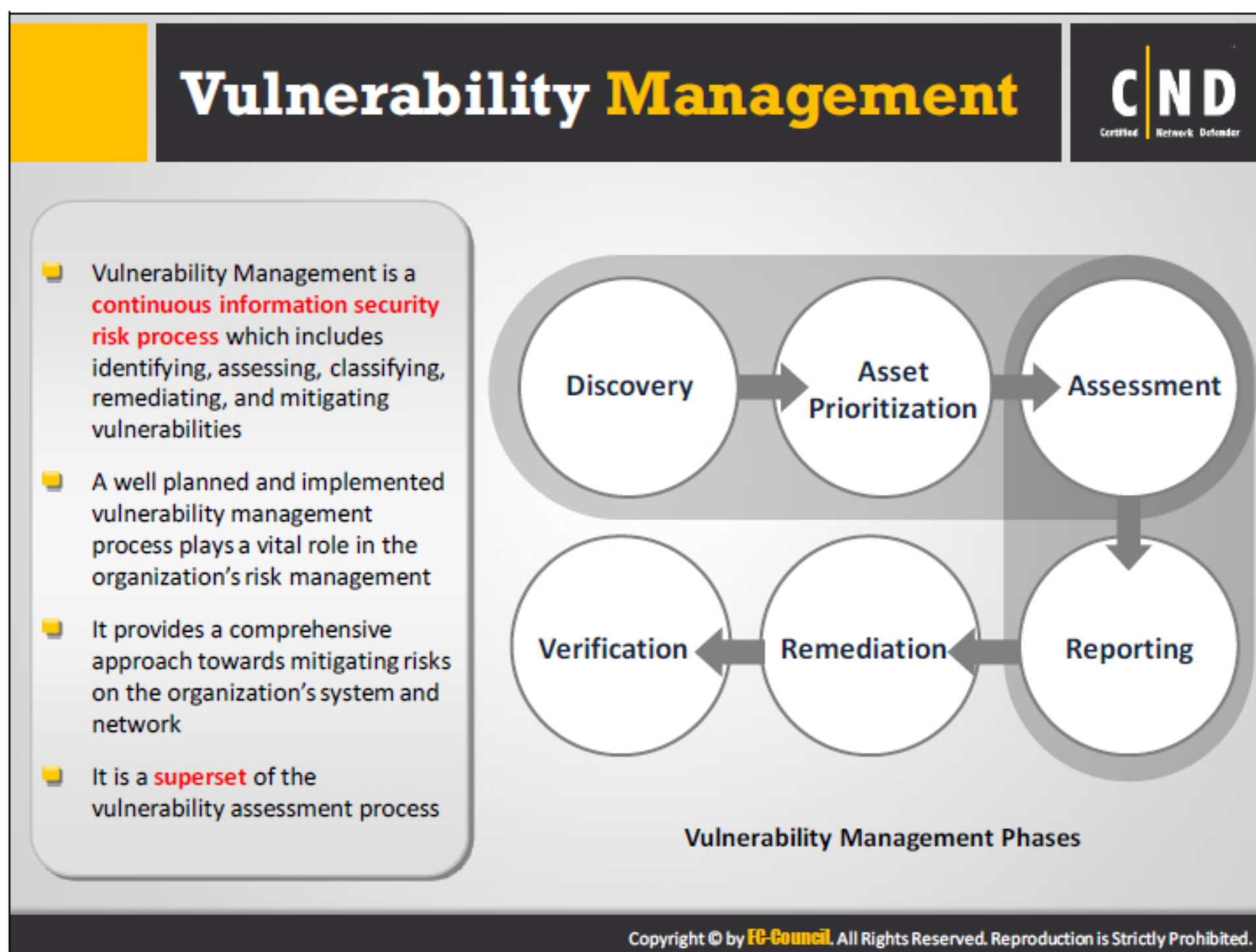


**CND**  
Certified Network Defender

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

<http://www.tripwire.com>

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



Vulnerability management deals with the continuous process of recognizing, evaluating, categorizing, removing and diminishing vulnerabilities. Vulnerability management may be done with the help of a vulnerability scanner by searching for vulnerabilities in a system.

Vulnerability management should be implemented in every organization as it evaluates and controls the risks and vulnerabilities in the system. The management process continuously examines the IT environments for vulnerabilities and risks associated with the system. The management process may be defined as:


- Draft vulnerability management policy.
- Identify the existing vulnerabilities.
- Evaluate the vulnerabilities, according to their priorities and provide required actions.
- Reduce the impact of the vulnerability on the system.
- Continue the process of evaluating the vulnerabilities and risks.

There are six levels in the vulnerability management phases. Every process concentrates on improving the security risks of the network.

## The six levels in vulnerability management include:


- **Discovery (Mapping):** A phase in which the network assets are identified, considered and evaluated.
- **Asset prioritization (and Allocation):** Risks are compared against a predefined set of features and assigned a priority.
- **Assessment (Scanning):** Scan and evaluate the systems for vulnerabilities.
- **Reporting (Technical and Executive):** Reports the results achieved for the different vulnerability management processes.
- **Remediation (Treating risks):** Reduce the risks in the vulnerability and remove the root cause.
- **Verification (Rescanning):** Continuous monitoring of the network to check for new vulnerabilities.

## Discovery - Identify the Components of a Network



### Discovery using Qualysguard Vulnerability Management

- In this phase, all the network components and assets are identified
- Network discovery will help you detect **rogue** devices on the network
- Provides a **hacker's view** of the network



The screenshot shows the Qualysguard interface. On the left, a table lists discovered hosts with columns for IP address, hostname, and status. The table includes 15 hosts, with the first one highlighted. On the right, a network map visualizes the discovered hosts and their connections. Below the map, a 'Preview' section shows details for a selected host, including its IP address, hostname, and operating system.

IP Address	Hostname	Status
10.15.10.16	ip-10-15-10-16.us-east-1.elb.amazonaws.com	Up
10.15.10.35	ip-10-15-10-35.us-east-1.elb.amazonaws.com	Up
10.15.10.37	ip-10-15-10-37.us-east-1.elb.amazonaws.com	Up
10.15.10.38	ip-10-15-10-38.us-east-1.elb.amazonaws.com	Up
10.15.10.49	ip-10-15-10-49.us-east-1.elb.amazonaws.com	Up
10.15.10.41	ip-10-15-10-41.us-east-1.elb.amazonaws.com	Up
10.15.10.42	ip-10-15-10-42.us-east-1.elb.amazonaws.com	Up
10.15.10.43	ip-10-15-10-43.us-east-1.elb.amazonaws.com	Up
10.15.10.45	ip-10-15-10-45.us-east-1.elb.amazonaws.com	Up
10.15.10.46	ip-10-15-10-46.us-east-1.elb.amazonaws.com	Up
10.15.10.47	ip-10-15-10-47.us-east-1.elb.amazonaws.com	Up

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

An inventory detailing the assets is created and later identifies the host details in order to identify vulnerabilities. An automated scheduled check for vulnerabilities is performed.

The basic steps in the Discovery phase are:

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

You can use automated network discovery tools to identify the network components, for example, you can use Qualysguard Vulnerability Management to perform network discovery.

This tool will help you:

- **Mapping the network:**

Provides a graphical host explaining the details of the network.


- **Assign each asset to the business:**

Assign the identified assets, according to the business needs. Help in categorizing the approaches and reducing the effect of a vulnerability in the network.

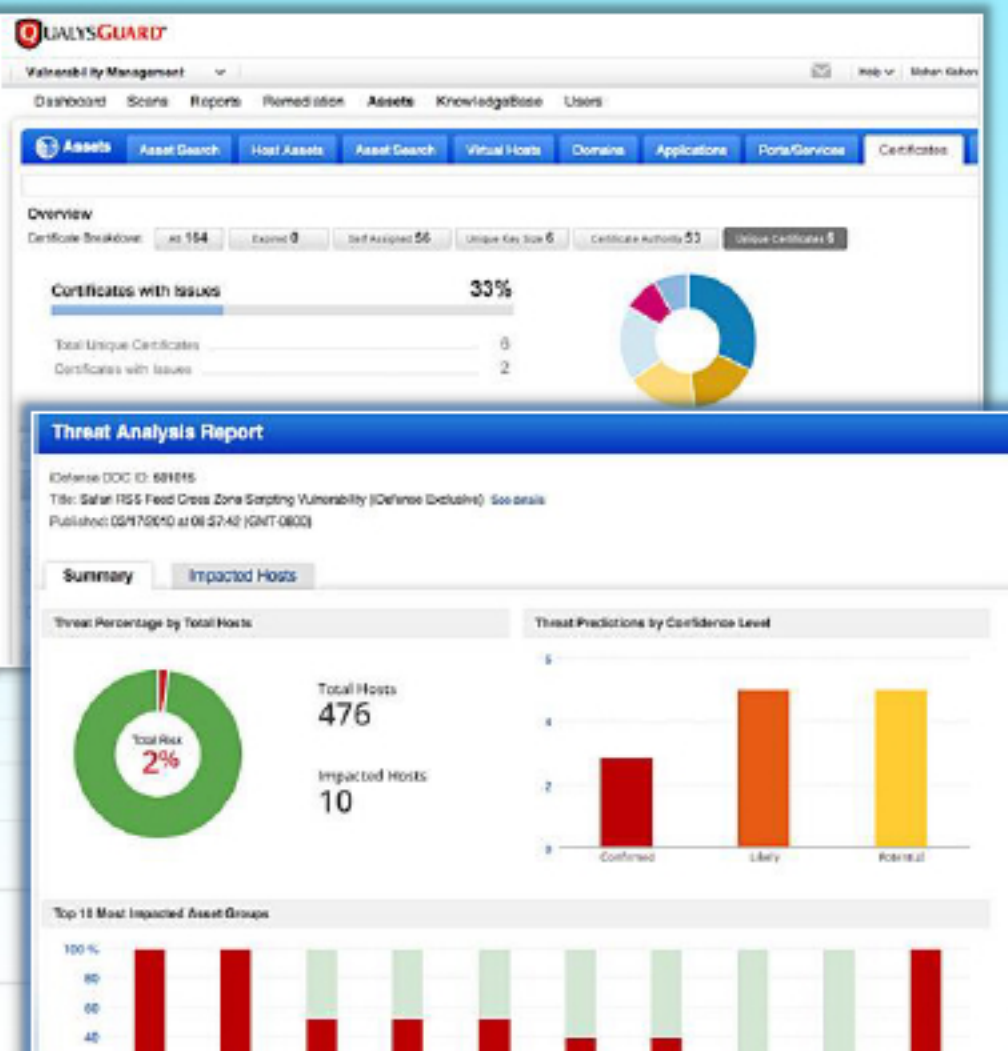
- **Identify the ports, OS, services and certificates on each device:**

Provides details regarding the identified operating system, open ports available and the certificates installed on each device.

## Asset Prioritization - Evaluate the Importance of each component



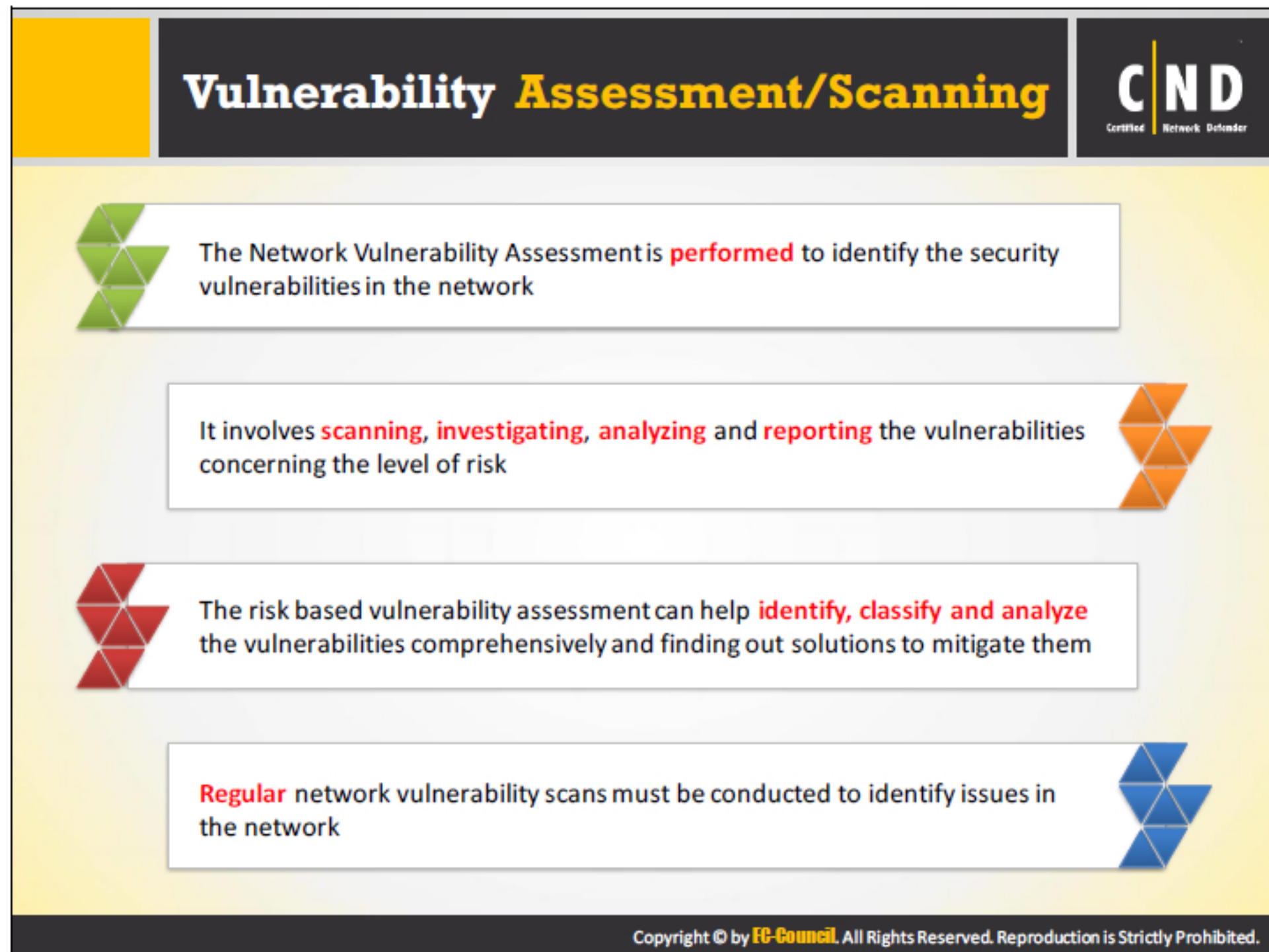
- Asset prioritisation helps create a **customized list** of what to tackle first, second, third and so on
- Identify the assets which are more **critical** to the business
- Identify the value for each specific asset
- Criticality of the assets depend on the business impact



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

Classify the identified assets, according to the business needs. Classification helps in identifying the high business risks in an organization. Prioritize the rate assets based on the impact of their failure and on the reliability of those assets in the business. Prioritization helps:

- Evaluating and deciding a solution for the consequence of the assets failing.
- Examining the risk tolerance level.
- Organizing the methods for prioritizing the assets.



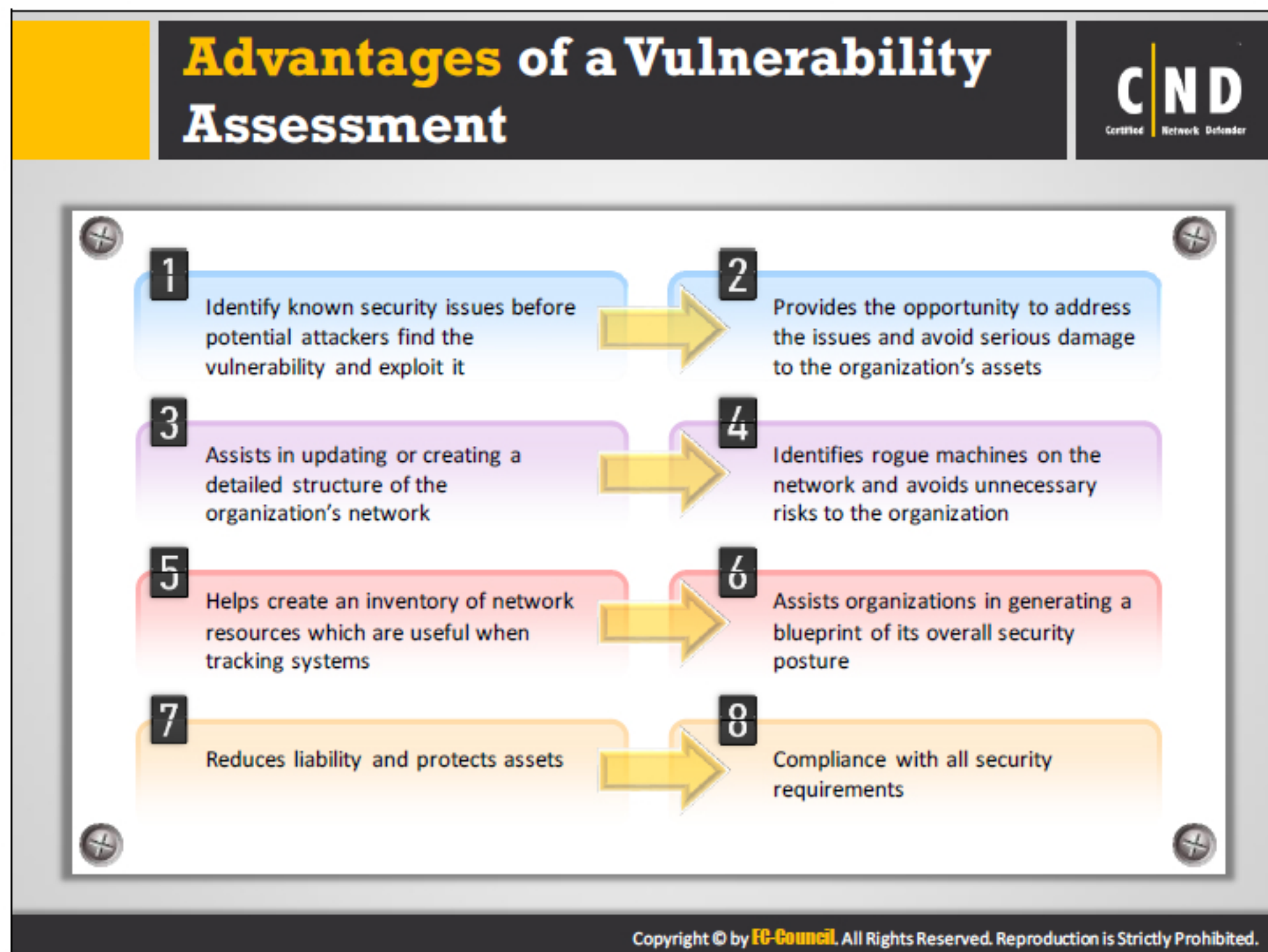
A vulnerability assessment is the process of identifying vulnerabilities in network components, including the operating system, web applications, web server, etc. It helps identify the category and criticality of the vulnerability in an organization. The organization rates the vulnerabilities and prioritizes them design methods to remedy the situation accordingly. The assessment method helps measure the effectiveness of those remedies.

The ultimate goal of vulnerability scanning includes scanning, examining, evaluating and reporting the vulnerabilities in the network. It helps minimize the levels of risk to the organization. There are many steps involved in a vulnerability assessment:

- Classify the 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.

Vulnerability scans when performed at regular intervals are beneficial in locating any issues and in selecting an appropriate security control to mitigate those issues. Doing this on a regular basis, reduces the risk to a great extent.

There are automated tools available for vulnerability scanning, including Nessus, SAINT, OpenVAS, and Nikto.



Organizations perform a network vulnerability assessment in order to detect and eradicate vulnerabilities in the network. It manages the risk to the organization. All network components are assessed against possible vulnerabilities during regular intervals. A vulnerability assessment will help:

- Identify 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.

**Requirements for an Effective Network Vulnerability Assessment**

**CND**  
Certified Network Defender

Consider the following for an effective vulnerability assessment:

- Ability to identify the assets that require a vulnerability scan
- Check the vulnerability scanning tools for any false positives
- Select the assessment tools which will cause the least network disturbance
- Maintain a change control system during the vulnerability scan, to keep track of all activities
- Effective assessment tools include features such as trending, reporting and remediation tracking

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

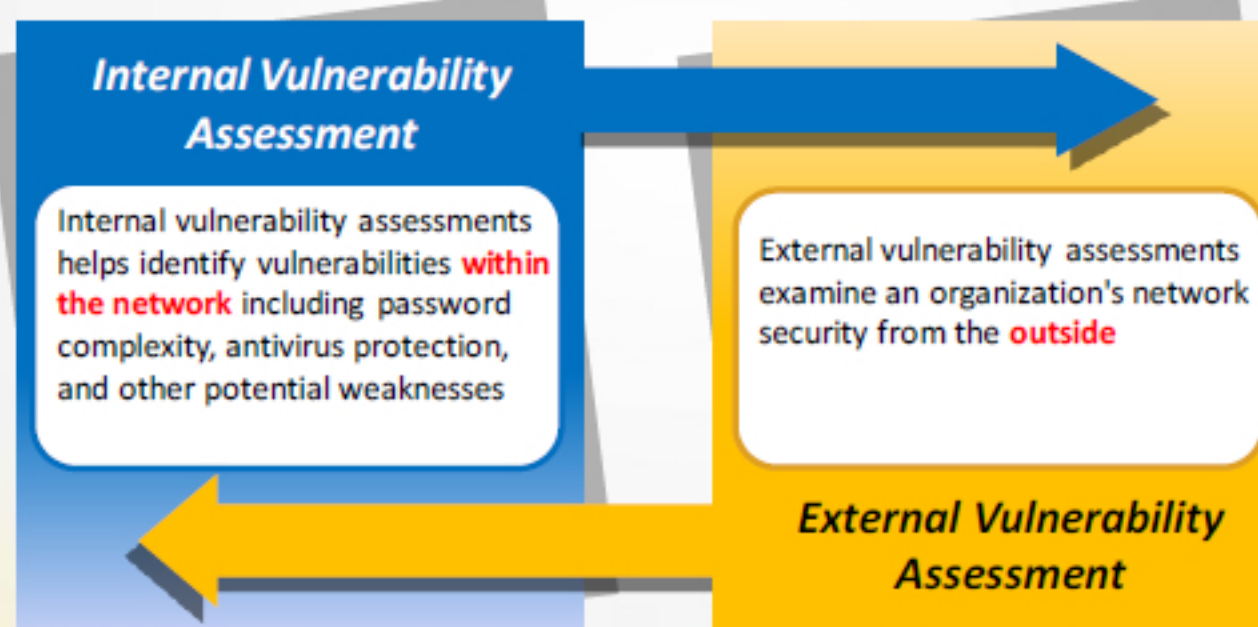
Conducting a vulnerability assessment at regular intervals is required for an effective network vulnerability assessment. To conduct a vulnerability assessment more effectively, administrators need to consider the following points:

- Identify what assets of the network should be assessed for vulnerabilities. Identify the assets and evaluate its criticality is important to minimize any potential risks to the assets.
- Check the vulnerability scanning tools for false positives when receiving the assessment results. Identified vulnerabilities may be a false positive. It is very important to validate the identified vulnerability as genuine. To do this, perform a vulnerability assessment with a variety of tools. Do not depend on a single tool for the vulnerability scanning assignment.
- Choose assessment tools which cause minimal network disturbances. Vulnerability assessment tools can create a serious impact on network performance during an assessment. Choose only the appropriate tools to get the job done and those which do not cause additional issues with network performance.
- Use a change control system to keep track of all the activities during a vulnerability scan.
- Only consider assessment tools with key features such as trending, reporting and remediation tracking.

## Types of Vulnerability Assessments



- Understand the design of the network and the systems before conducting a vulnerability assessment
- Network performance can be degraded or even stop functioning due to vulnerability assessments



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

## Example: Internal and External Vulnerability Assessments



### Internal vulnerability examples:

- ⓘ **Ineffective Procedures:** Ineffective security configuration procedures in a network
- ⓘ **Old Passwords:** Accounts with passwords older than one month
- ⓘ **Old Patch Levels:** Available patches and updates

### External vulnerability examples:

- ⓘ **FTP Anonymous Access :** A perimeter security review to check if the server permits anonymous access to accounts for terminated employees
- ⓘ **Email Relay:** Checks the server for open relay emails

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

There are two types of network vulnerability assessments:

- **Internal Vulnerability:** Examines the security of the internal network.
- **External Vulnerability:** Examines the security of the servers facing the Internet.

A complete understanding of the design of the network and the system is required before performing a vulnerability assessment. There are instances where the vulnerability assessment may affect the network, causing a performance degradation or even preventing it from functioning properly.

### Internal Vulnerability Assessment

An internal vulnerability assessment recognizes the vulnerabilities in the network. This includes password complexity, antivirus protection used, etc. An internal assessment evaluates the network for the presence of internal vulnerabilities. Conduct a vulnerability assessment on every critical device to identify all possible vulnerabilities, which an attacker will exploit. Internal assessments create a report based on the vulnerabilities detected in the network.

The internal vulnerability assessment includes:

- **Host and service discovery:** Discovering all accessible systems and services running. This 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.

### External Vulnerability Assessment

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

The following actions are performed during an external vulnerability assessment:

- Find all hosts on the network.
- Fingerprint their operating systems.
- Detect open ports on the system.
- Map the ports to various network services.
- Detect the version of all the 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 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.

## 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.
- **E-mail Relay:** Checking whether the email server allows open email relaying.

## Steps for an Effective External Vulnerability Assessment



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

1. Find the **live hosts** on a network
2. Perform **OS Fingerprinting** on the detected hosts
3. Detect **open ports** on the target system
4. Map open ports and running **services**
5. Find the **version** of all the running services
6. Map the **service version** with the security vulnerabilities which are associated
7. Check if the **service** is vulnerable or if it has been patched

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

The process of a vulnerability assessment undergoes the following four stages:

1. Plan and configure the vulnerability assessment
2. Setting up the tasks to run and generate the reports
3. Resolve the vulnerabilities
4. Maintain a security baseline for the network

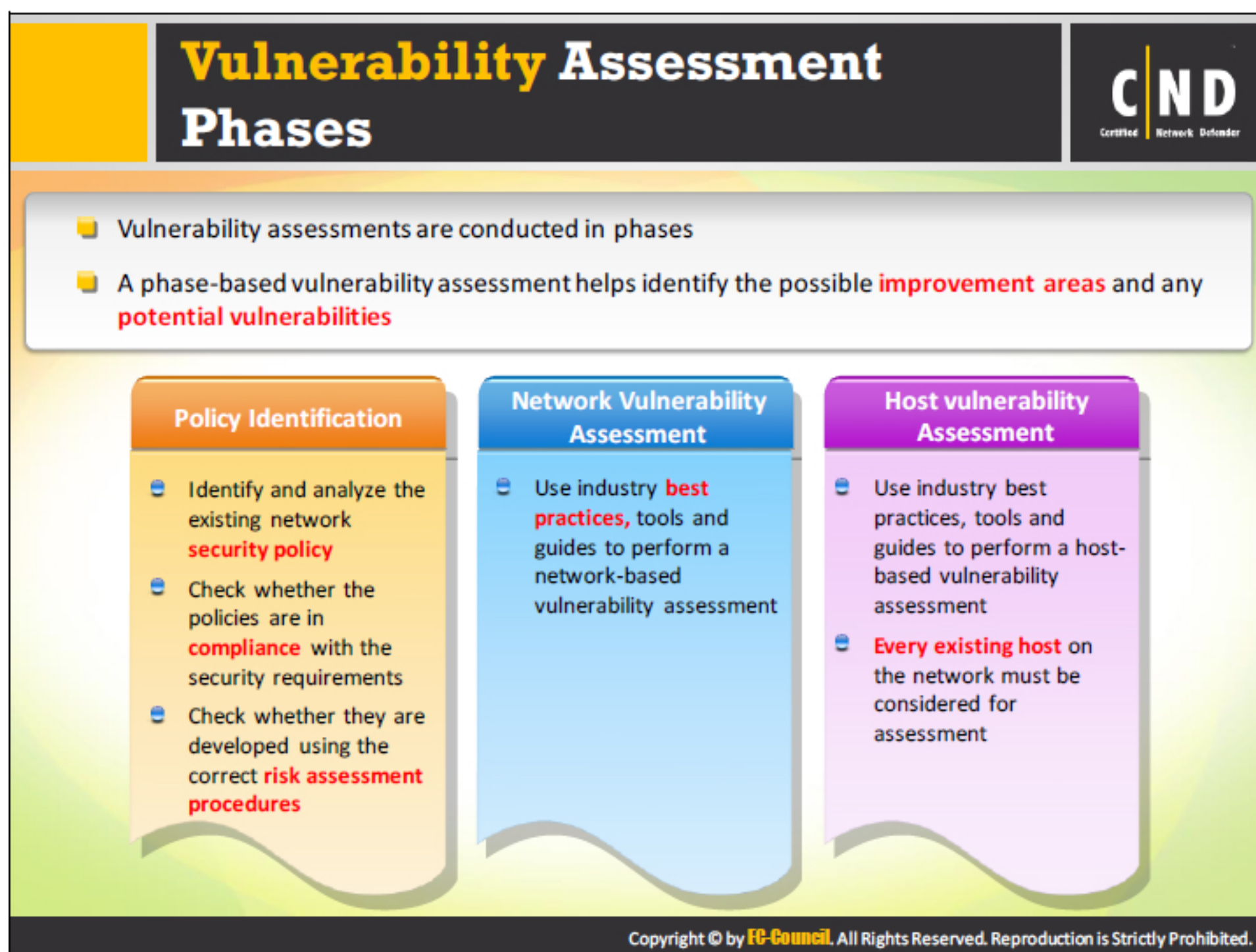
### Guidelines for an effective External Vulnerability Assessment

- Regularly perform an external vulnerability assessment. The assessment includes all the devices in the network, including new ones. Vulnerabilities detected in one device or a system does not conclude the entire network is corrupt. However, the need to optimize the 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 the open ports and interfaces and take action accordingly.
- Avoid conducting a vulnerability assessment on a particular device or a system. The vulnerability assessment should be applicable for all the devices in the network. Determine the status of the services running on the system. Unpatched applications can be vulnerable to attacks. Patch any application or service that is not patched and requires an update.

- Map the network infrastructure, connecting the hardware together to boost the network and application performance.

**Typical tasks executed for an effective External Vulnerability Assessment are:**

- Collect all information related to a network.
- Collect and document everything, including all the information 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 the weak user authentication systems.



A vulnerability assessment is a highly complex procedure for administrators, depending on the version and the configuration of the network setup. The network environment is dynamic and an administrator may implement the vulnerability assessment phases below.

▪ **Policy Identification:**

In this phase, the administrator is required to understand the security policy of the organization. Based on the security policy identification, they will determine if the policy is in adherence with the current network infrastructure. After reviewing the organization's policy, the administrator will be able to detect the location(s) where vulnerabilities exist and what type of vulnerability assessment is required to be performed.

▪ **Network Vulnerability Assessment:**

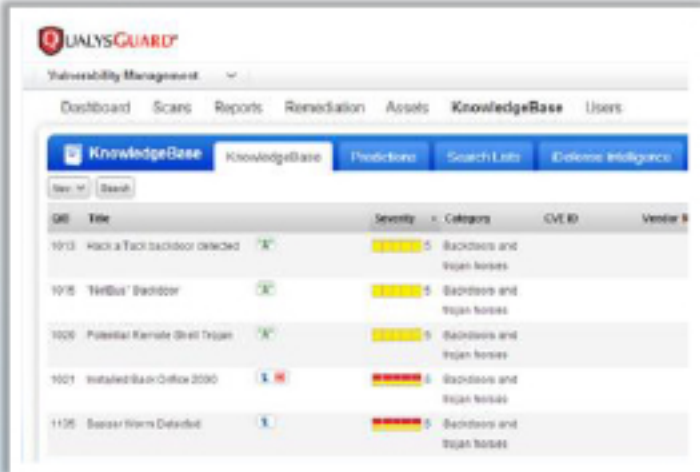
The administrator has to determine the non-functional or suspicious network devices that can compromise the normal function of the system. In this phase, the administrator investigates and analyzes the risk associated with the detected vulnerability and takes the appropriate action. With the help of certain network scanning and vulnerability tools the administrator will assess:

- Security control checks.
- Identifying, analyzing and prioritizing network threats.
- Password analysis of network devices.

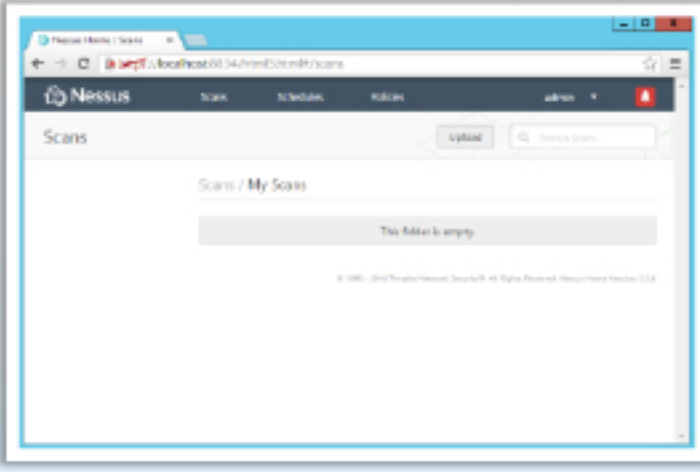
- Determining the network strength.
- **Host Vulnerability Assessment:**

Involves assessing the system or the account of a local user. In this phase, the administrator checks the configuration settings for the system. They detect the accounts with weak or old passwords, suspicious files in the system, modifications in the system settings, etc. The main advantage of a host vulnerability assessment is that it allows the administrator to assess every file present in the system.

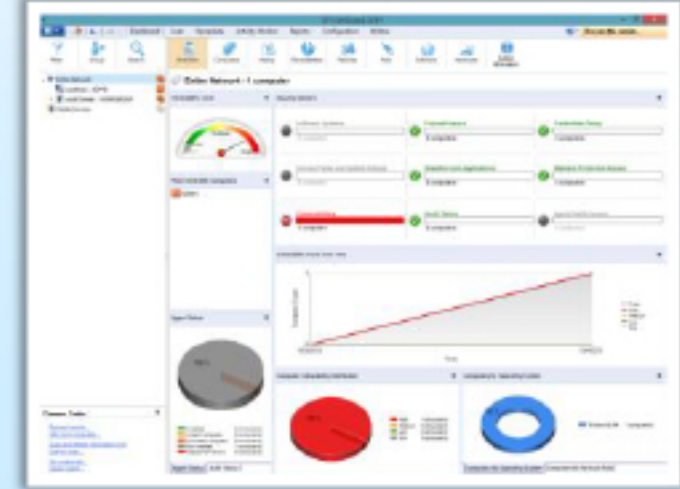
# Network Vulnerability Assessment Tools



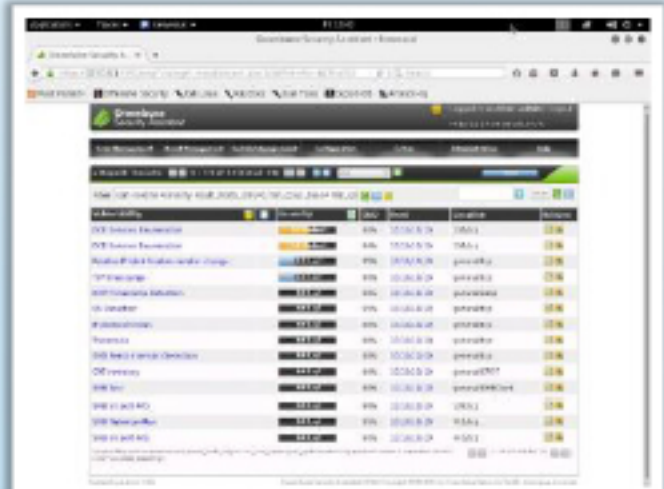
**Network Vulnerability Assessment using QualysGaurd**  
(<https://www.qualys.com>)



**Network Vulnerability Assessment using Nessus**  
(<https://www.tenable.com>)



**Network Vulnerability Assessment using GFI LanGuard**  
(<http://www.gfi.com>)



**Network Vulnerability Assessment using OpenVAS**  
(<http://www.openvas.org>)

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

## QualysGaurd

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

Qualysguard helps in protecting the IT infrastructure in accordance with the company policies and procedures. It identifies the internal threats and develops methods required to protect the network. Features of Qualysguard network vulnerability tool are:

- It identifies the operating system, open ports, active services running on a system.
- Examines the network continuously for any changes.
- Provides an approach in order to prioritize the remediation steps.
- Assists with scanning the internal network for vulnerabilities.
- Provides reports to the user in order to understand the security of the network.

## Nessus

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

A vulnerability scanner that scans the following types of vulnerabilities:

- Hackers getting access to important data in the system.
- Misconfiguration.
- Password attack.

- Denial of service against the TCP/IP stack.
- Preparation of PCI DSS audits.

**Features of Nessus include:**

- Scanning provides the real time values and no need to wait for the scanning to be completed in order to view the results.
- Provides the same user interface for all operating systems, including Mac, Windows, and Linux.
- Scanning continues in the server even if the UI is disconnected.
- Provides a scan template that creates scan policies for auditing the network.

**GFI LanGuard**

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

GFI LanGuard scans your operating systems, virtual environments and installed applications through vulnerability check databases such as OVAL and SANS Top 20. GFI LanGuard enables you to analyze the state of your network security, identify risks and address how to take action before it is compromised.

A proper network analysis to determine the state of your network is another essential step to reduce the risks to the network, determine its degree of exposure, and address how to take action before it is compromised.


GFI LanGuard is able to scan for over 60,000 vulnerabilities across your network, including virtual environments, mobile and network devices.










**OpenVas**

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

OpenVAS provides a comprehensive and powerful vulnerability scanning and vulnerability management solution. OpenVAS receives support and contributions from many individuals and organizations, adding to the quality and reliability of the solution: penetration testers, power users, security researchers, academia etc.

## Additional Vulnerability Assessment Tools



 <b>Retina CS</b> <a href="http://www.beyondtrust.com">http://www.beyondtrust.com</a>	 <b>Acunetix Online Vulnerability Scanner (OVS)</b> <a href="http://www.acunetix.com">http://www.acunetix.com</a>
 <b>Core Impact Professional</b> <a href="http://www.coresecurity.com">http://www.coresecurity.com</a>	 <b>Security Manager Plus</b> <a href="http://www.manageengine.com">http://www.manageengine.com</a>
 <b>MBSA</b> <a href="http://www.microsoft.com">http://www.microsoft.com</a>	 <b>Nexpose</b> <a href="http://www.rapid7.com">http://www.rapid7.com</a>
 <b>Shadow Security Scanner</b> <a href="http://www.safety-lab.com">http://www.safety-lab.com</a>	 <b>SAINT</b> <a href="http://www.saintcorporation.com">http://www.saintcorporation.com</a>
 <b>Nsauditor Network Security Auditor</b> <a href="http://www.nsauditor.com">http://www.nsauditor.com</a>	 <b>AlienVault Unified Security Management™ (USM)</b> <a href="https://www.alienvault.com">https://www.alienvault.com</a>

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

### Retina CS

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

Retina CS provides organizations with context-aware vulnerability assessment and risk analysis. It identifies security exposures, analyzes business impact, plans and conducts remediation across disparate and heterogeneous infrastructure. Features of Retina CS include:

- Discover network, web, mobile, cloud and virtual infrastructure
- Profile asset configuration and risk potential
- Pinpoint vulnerabilities, malware and attacks
- Analyze threat potential and return on remediation
- Remediate vulnerabilities via integrated patch management (optional)
- Report on vulnerabilities, compliance, benchmarks, etc.
- Protect endpoints against client-side attacks

### Core Impact Professional

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

Core impact professional helps:

- Leverage true multi-vector testing capabilities across network, web, mobile, and wireless

- Test with 25% more unique Common Vulnerability Exploits (CVE)
- Validate patching efforts to ensure vulnerabilities were remediated correctly

## **MBSA**

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

MBSA identifies missing security updates and common security misconfigurations. MBSA includes a graphical and command line interface that can perform local or remote scans of Microsoft Windows systems.

## **Shadow Security Scanner**

Source: <http://www.safety-lab.com>

Shadow security scanner provides a secure, prompt and reliable detection of a vast range of security system holes. It analyzes the data collected, locates vulnerabilities and possible errors in server tuning options and suggests possible solutions.

## **Nsauditor Network Security Auditor**

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

Nsauditor Network Security auditor scans networks and hosts for vulnerabilities, and provides security alerts. It reduces the total cost of network management in enterprise environments by enabling IT personnel and systems administrators to gather a wide range of information from all computers in the network, without installing server-side applications on these computers and it creates a report of potential problems found.

## **Acunetix Online Vulnerability Scanner (OVS)**

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

Acunetix Online Vulnerability Scanner acts as a virtual security officer. It helps you scan websites, including integrated web applications, web servers and any additional perimeter servers for vulnerabilities. And allowing you to fix them before hackers exploit the weak points in your IT infrastructure.

## **Security Manager Plus**

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

A network security scanner, that proactively reports on network vulnerabilities and helps remediate them by ensuring compliance. Security Manager Plus protects the network from security threats and malicious attacks using vulnerability scanning, open ports detection, patch management, Windows file/folder/registry change management and vulnerability reporting capabilities.

## **Nexpose**

Source: <http://www.rapid7.com>

Nexpose provides assessment solutions for your physical, virtual, mobile, and cloud environments. It supports the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting and mitigation.

## **SAINT**

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

SAINT uncovers areas of weakness and recommends fixes. SAINT scanner includes:


- Identify vulnerabilities on network devices, operating systems, desktop applications, Web applications, databases, and more.
- Detect and fix possible weaknesses in the network's security before they can be exploited by intruders.
- Anticipate and prevent common system vulnerabilities.
- Demonstrate compliance with current government and industry regulations such as PCI DSS, NERC, FISMA, SOX, GLBA, and HIPAA.
- Perform configuration audits with policies defined by FDCC, USGCB, and DISA.

## **AlienVault Unified Security Management (USM)**

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

AlienVault USM provides built-in vulnerability assessment with the essential capabilities you need for complete security visibility and threat intelligence.

## Choosing a Vulnerability Assessment Tool



Administrators should consider the following factors while choosing a vulnerability assessment tool:

- ❖ Vulnerability scanners cannot identify vulnerabilities when its **plug-in is outdated**
- ❖ Choose a scanner with an **auto-update feature**
- ❖ Check the tool's **accuracy** and **capability** in identifying critical vulnerabilities
- ❖ A vulnerability scanner should be capable of producing a report of the scanned and detected vulnerabilities
- ❖ A tool with a **back-end database** assists administrators with performing assessments

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

There are various vulnerability assessment tools available in the market. Multiple tools should be identified as several different products are needed to evaluate the network environment. Evaluate each product based on the quality and speed of updates, compatibility with the environment, support for cloud services, compliance, prioritization, active and passive detection, authenticated and unauthenticated scanning, remediation guidance and vendor support.


The selection of an appropriate vulnerability assessment is done based on the how it works, key features such as expertise, accuracy, reliability, scalability and reporting.

The following points will help make the best selection:

- Scanners will find the vulnerabilities at a faster rate with the help of updated plug-ins.
- Scanners with an auto-update feature are best suited for vulnerability scanning.
- The identified vulnerability accuracy will be concentrated more than the amount of vulnerability checks which are completed.
- The scan report will provide all the details so any problems can be examined and solved. By comparing the scan results, vulnerability trends will be understood.
- Check if the tool is compatible with the applications, operating systems and infrastructure components.
- Distinguish between authenticated and unauthenticated scanning.

- What solutions does the tool provide after vulnerabilities are identified?
- Can security managers identify the issues with the configuration?

## Choosing a Vulnerability Assessment Tool: Deployment Practices and Precautions



Network operators should consider the following issues before conducting a vulnerability assessment:

Deployment Practices	Precautions
<ul style="list-style-type: none"><li>Place a vulnerability scanner in front of the <b>firewall</b></li><li>Consider including a port scan in the vulnerability assessment</li><li>It is recommendable to keep archived logs of all vulnerability assessments and compare them with the latest results</li><li>Correctly interpret the assessment results to identify valid vulnerabilities and fix them</li></ul>	<ul style="list-style-type: none"><li>A risk assessment along with careful planning are necessary before conducting a vulnerability assessment</li><li>It is important to <b>safeguard</b> the assessment results by encrypting them to prevent unauthorized access</li><li><b>Policies</b> and <b>procedures</b> should be defined and in place for the use of the vulnerability assessment tools</li></ul>

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

The following are the recommended deployment practices and precautions that are taken while selecting a vulnerability assessment tool:

### Practices


- **Location of the Scanner:** The scanners are placed inside or outside the firewall and must be monitored separately as they perform different actions.
- **Scanning Port-Range:** All the ports should be examined for vulnerabilities. Open ports are more susceptible to attacks. Scanning should include every port even those which are not specified.
- **Create a Baseline:** Every scan result should be logged to compare the results from previous scans. Logging is important as it helps check the effectiveness of the remedies applied after each scan.
- **Correct Interpretation:** The vulnerability scan results should be interpreted correctly as the remedy methods are implemented based on the results of the scan.

### Precautions

- **Risks in Scan Process:** High alert should be given to enabling plug-ins as they may affect the scan process. Network performance may be affected as many network requests and traffic is generated during the scan process.

- **Securing Scanning Results:** If the results of the scan are disclosed, attackers will have an easier time exploiting the vulnerabilities in the network. Take precautions with the results and properly handle them.
- **Proper Policies and Procedures:** Proper policies and procedures should be implemented while performing a scan. Proper vulnerability tools should be used to maintain the security of the network.

# Reporting



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

Reports summarize the assets discovered and the exposure of each based on the following criteria:

Geographic location


Business unit

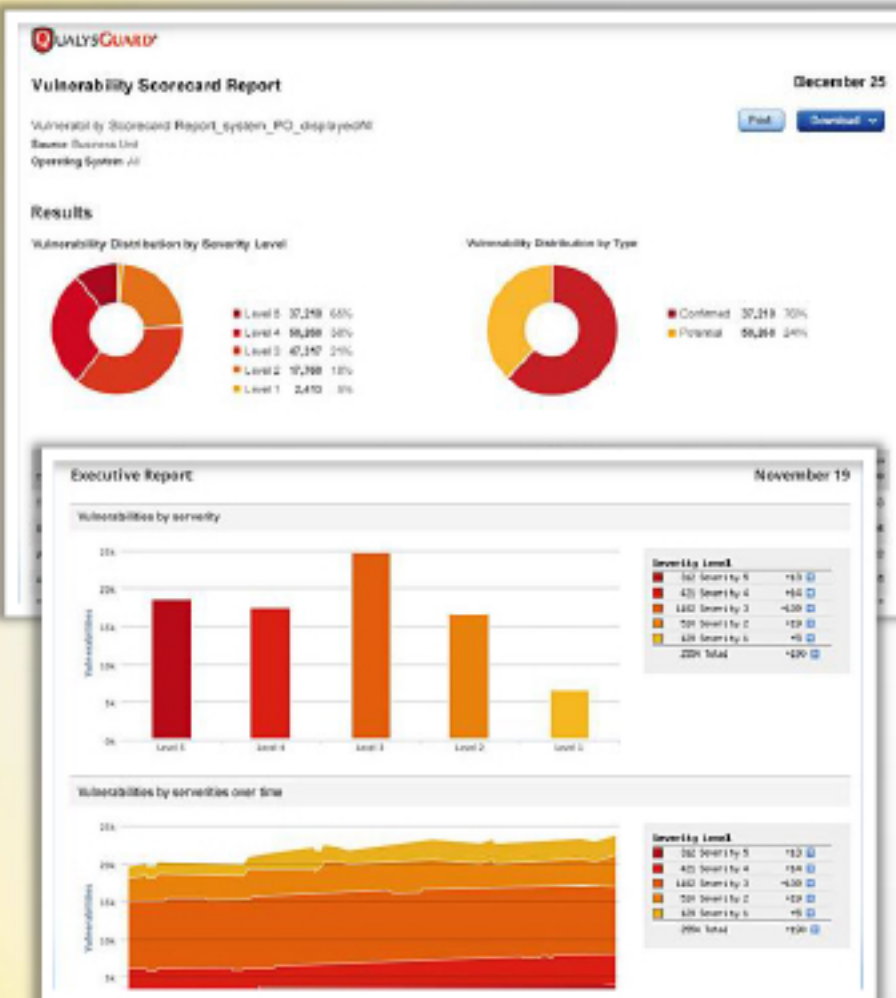
Goal category

Compliance area


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

# Vulnerability Management Report Examples





https://www.qualys.com



http://www.coresecurity.com

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

The important goals in creating a report are to provide a brief summary of what vulnerabilities exist in the network. Reporting enables security managers to prioritize and suggest proper remediation actions to deal with them.

**The report should contain the following details regarding the vulnerabilities found:**

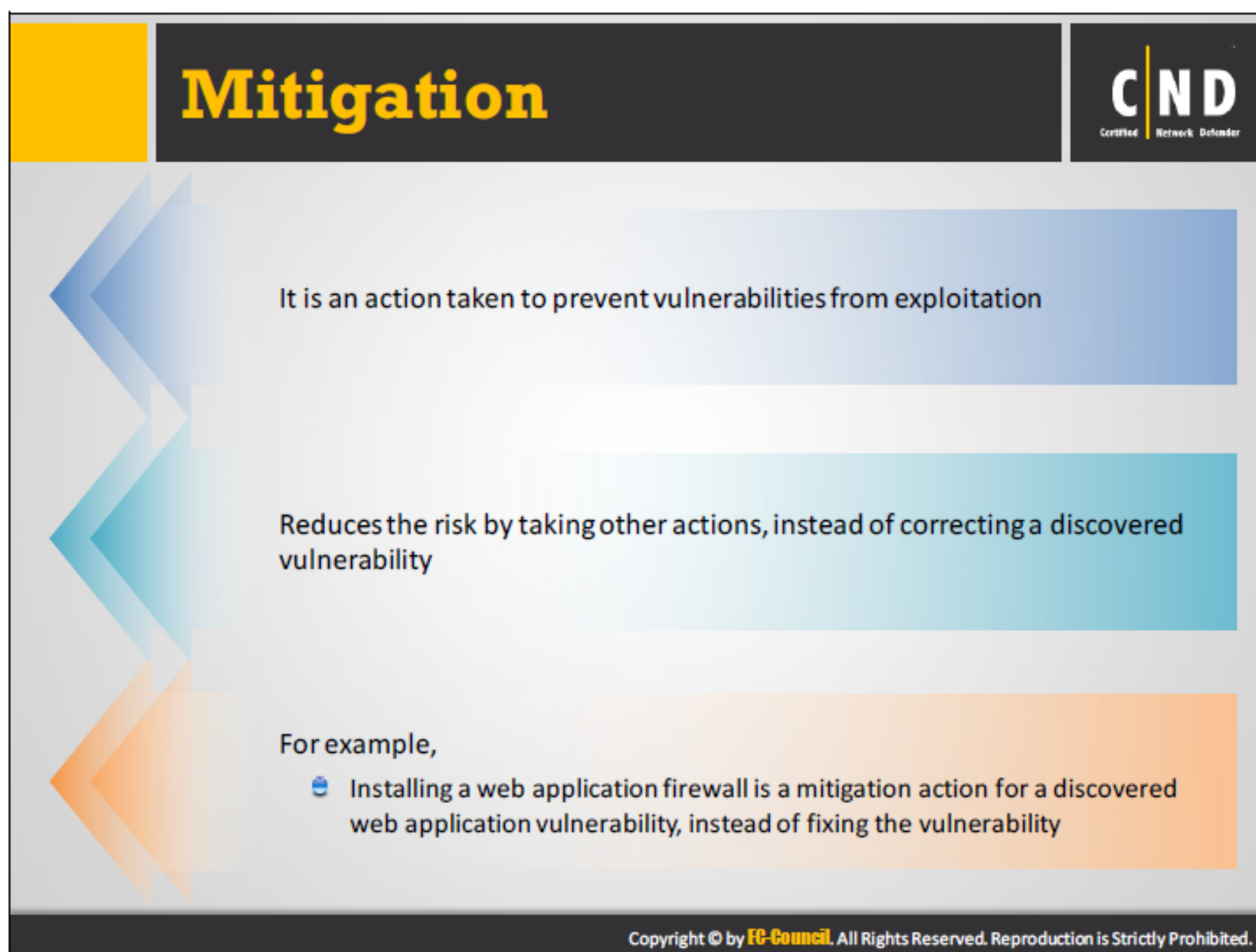
- Geographic Location
- Business unit
- Goal Category
- Compliance area

**The components of the report include:**

- Network assets included in the report
- Graphs and charts showing the status of the security
- Analysis of the trend in the network
- Details on the identified network

**Typical Anatomy of a Vulnerability Report:**

- Header
- Summary
- List of vulnerabilities - For each vulnerability, provide the following:
  - Unique tracking number
  - Risk level
    - High: Immediate action
    - Medium: Action required
    - Low: Action recommended
  - Brief description for each risk level identified
- Appendices - At a minimum the following two should be included:
  - Vulnerability details
  - Assessment setup

A slide titled "Mitigation" with a yellow header bar. The slide features three large, overlapping, semi-transparent arrows pointing to the right, each containing text. The top arrow is blue and contains the text "It is an action taken to prevent vulnerabilities from exploitation". The middle arrow is light blue and contains the text "Reduces the risk by taking other actions, instead of correcting a discovered vulnerability". The bottom arrow is orange and contains the text "For example," followed by a blue icon of a computer monitor and the text "Installing a web application firewall is a mitigation action for a discovered web application vulnerability, instead of fixing the vulnerability". The slide also includes a logo for "CND Certified Network Defender" in the top right corner and a copyright notice at the bottom: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

# Mitigation

CND  
Certified Network Defender

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 involves minimizing the risk of a vulnerability by performing certain actions. Mitigation may 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. Administrators should use appropriate mitigation strategies and techniques based on the vulnerability encountered.

Some examples of mitigation actions are:

- 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 the network from spoofing. A proper URPF mode should be configured before enabling this feature.
  - **IP source guard (IPSG):** It prevents IP traffic on non-routed, 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



**Remediation using Qualys Vulnerability Management (VM)**

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

Remediation is the process of fixing the identified vulnerabilities. Administrators should create a remediation plan and implement it to eradicate the discovered 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 all the way up to the network level.

### The remediation steps include:

- Confirm the created remediation is not based on a false positive.
- Create a prioritized list for the remediation.
- Create 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 include:

- Proper tools should be implemented for the vulnerabilities and the 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.

## Typical remediation tasks include:

### Action Plan:

- Budget
- Resources
- Priority
- Timing
  - Immediate
  - 30 Days
  - 6 Months
  - Future

### Typical Actions:

- Patch
- Upgrade
- Configuration Standards Rollout [by Role]
- Infrastructure Refresh
- New Deployment

**Verification**

CND  
Certified Network Defender


Perform another scan to ensure the vulnerability is **fixed** after the remediation process

Verifying the fixes ensures **compliance** with security


The verification should not **damage** any other network devices, services or applications

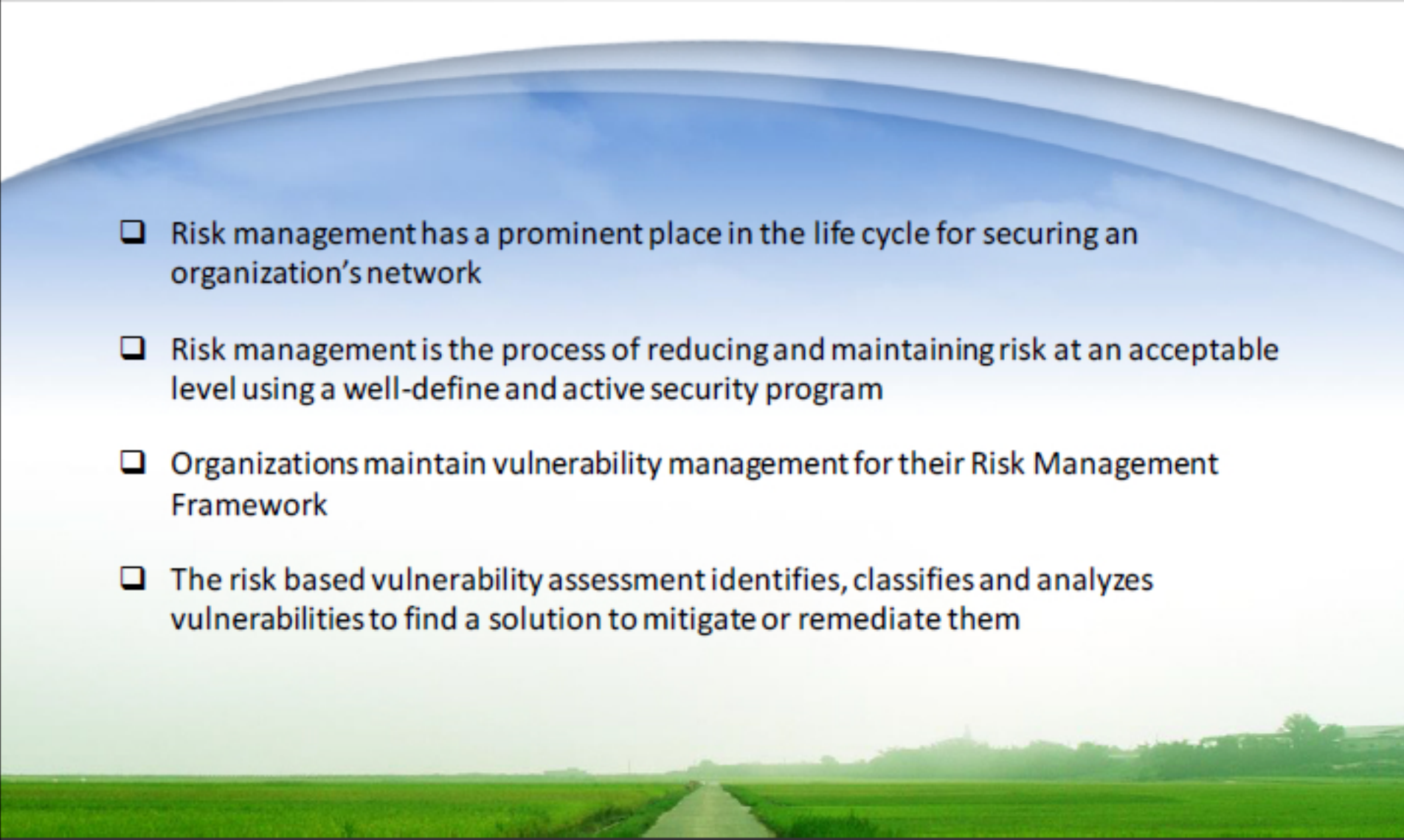
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Verifying the remediation ensures the vulnerabilities have been solved and fixed appropriately. After the remediation process concludes, scan for the vulnerability again. Perform an unlimited scan for all vulnerabilities which were originally discovered. Your vulnerability assessment will close upon verification of a successful remediation. Verification should not lead to the malfunction of any other network devices, services or applications. The vulnerability scan reports obtained after the fixes were verified ensures compliance with security provisions.



# 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
- ☐ Organizations maintain vulnerability management for their Risk Management Framework
- ☐ 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.

In this module, you have learned the risk and vulnerability management process. This module taught you the various phases involved in the risk and vulnerability management process. Vulnerability management helps you detect, assess, classify, remediate, and mitigate vulnerabilities and risks.

With this module, you will be able to conduct a systematic and phase-based vulnerability management of your network environment, with the help of automated vulnerability assessment solutions. These tools will help generate good vulnerability assessment reports for the organization.