EC-Council

C|CT

Certified | Cybersecurity Technician

Module - 22

Risk Management

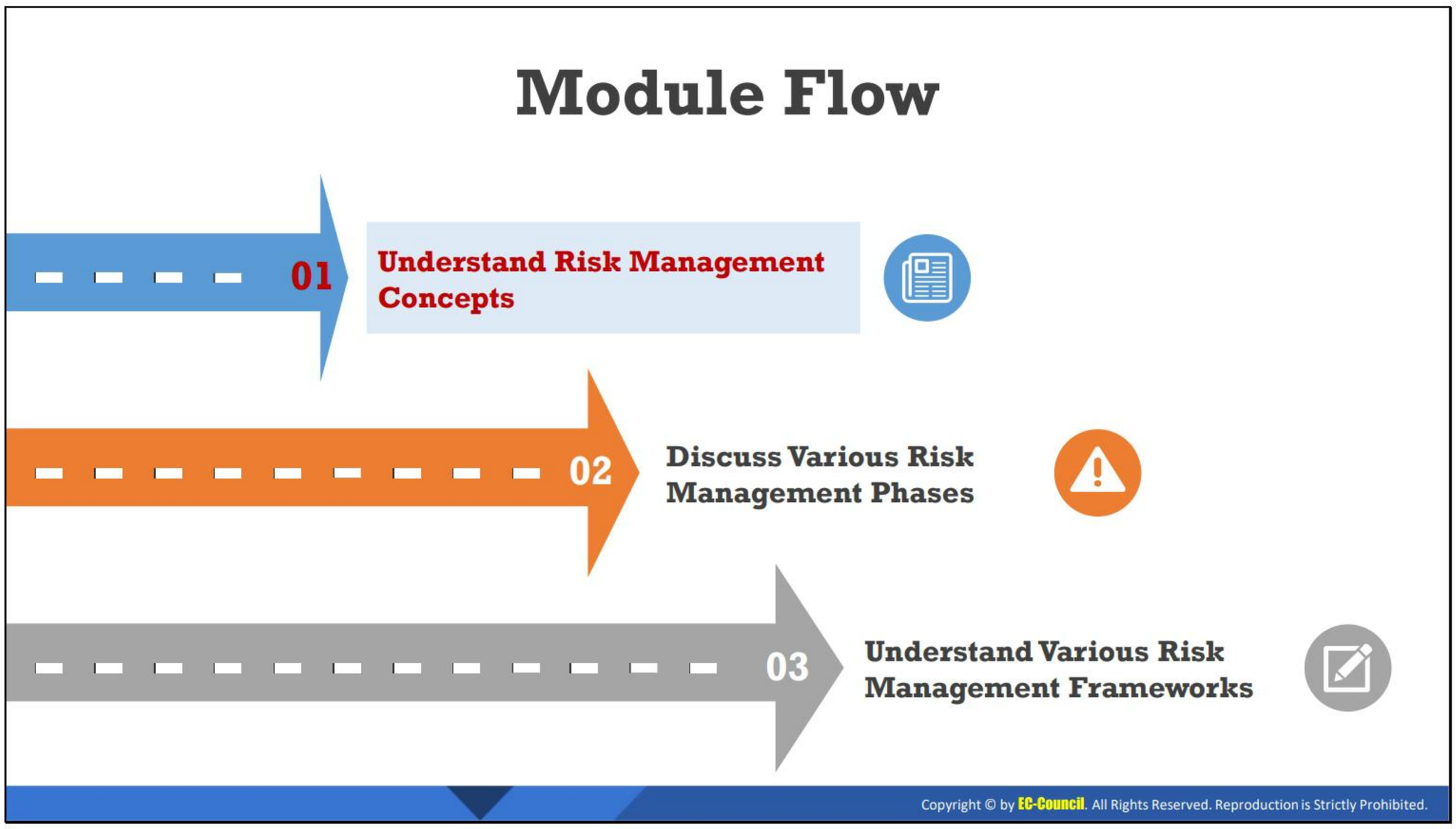
This page is intentionally left blank.

Module Objectives

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

At the end of this module, you will be able to do the following:

- Understand the concepts of risk management
- Describe different types of risks
- Explain various risk management phases
- Understand various risk management frameworks



Understand Risk Management Concepts

Risk and vulnerability management is a pro-active approach to manage network security. This section will introduce risk management concepts, key risk indicators (KRIs), key roles, and responsibilities in 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 the 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

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

Risk Management Objectives

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

Risk Management Benefits

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

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

Key Roles and Responsibilities in Risk Management

- **Senior Management**

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

- **Chief Information Officer (CIO)**

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

- **System and Information Owners**

  System and information owners mainly monitor the plans and policies developed for information systems. They are mainly responsible for implementing appropriate security controls to maintain confidentiality, integrity, and availability of an information system. Their responsibilities include the following:

  - Take part in all discussions on the configuration management process
  - Keep a record of the information system's components
  - Investigate all changes in the information systems and their impact
  - Prepare a security status report for all information systems

- Update the security controls required for protecting the information systems
- Update the security related documents on a regular basis
- Examine and evaluate the existing security controls in order to confirm their efficiency in protecting a system

- **Business and Functional Managers**

  They are responsible for maintaining all management processes in an organization. They are empowered with the authority to manage almost all processes in an organization. They responsible for making trade-off decisions in the risk management process. The roles defining functional managers are:

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

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

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

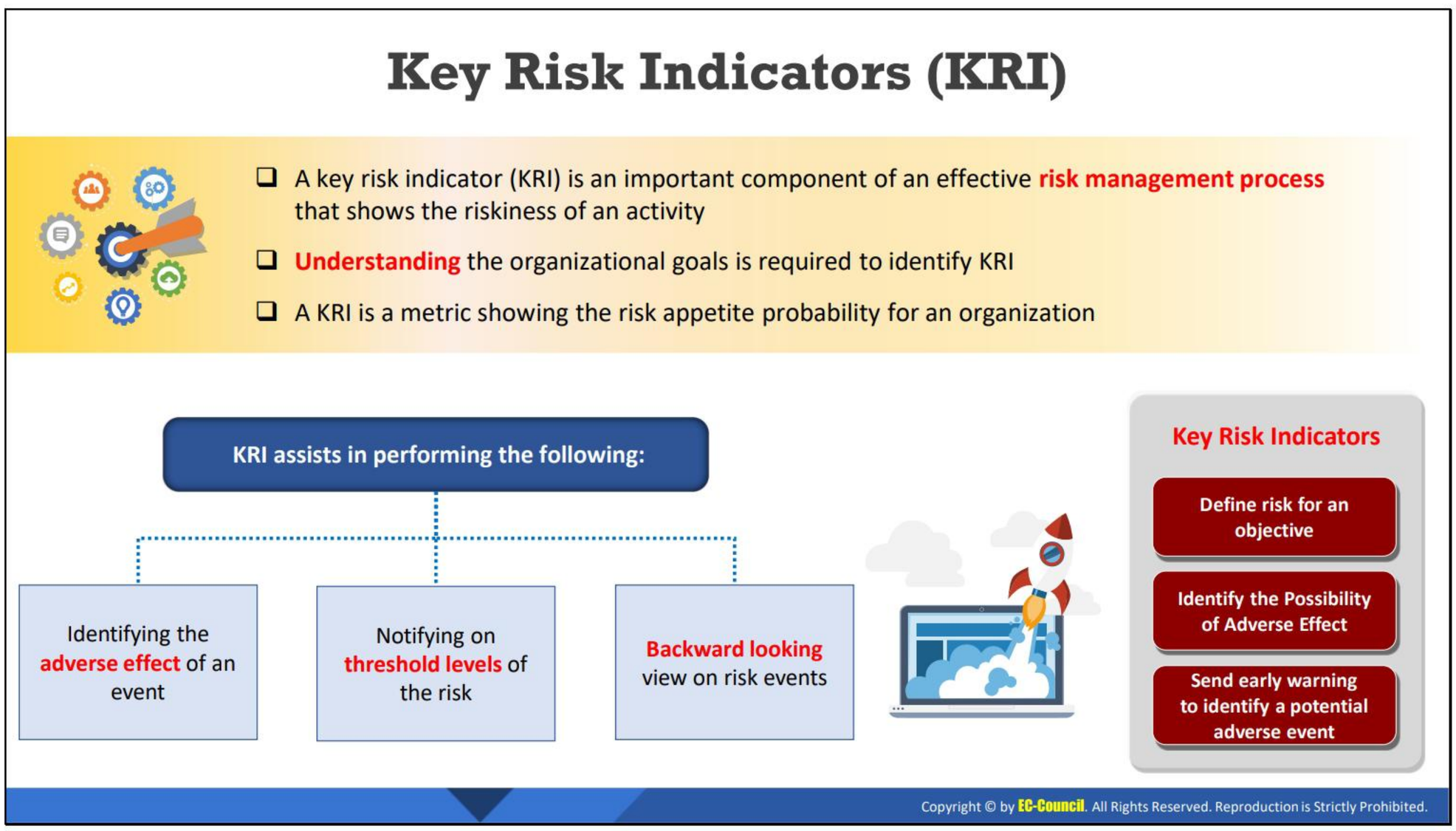
- **IT Security Practitioners**

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

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

- **Security Awareness Trainers**

  Security awareness trainers provide IT security awareness and training programs in an organization. They are often subject matter experts and ensure that only proper content is included in the program. They are mainly responsible for developing and providing appropriate training in the risk management process.



Key Risk Indicators (KRI)

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

Role of KRIs

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

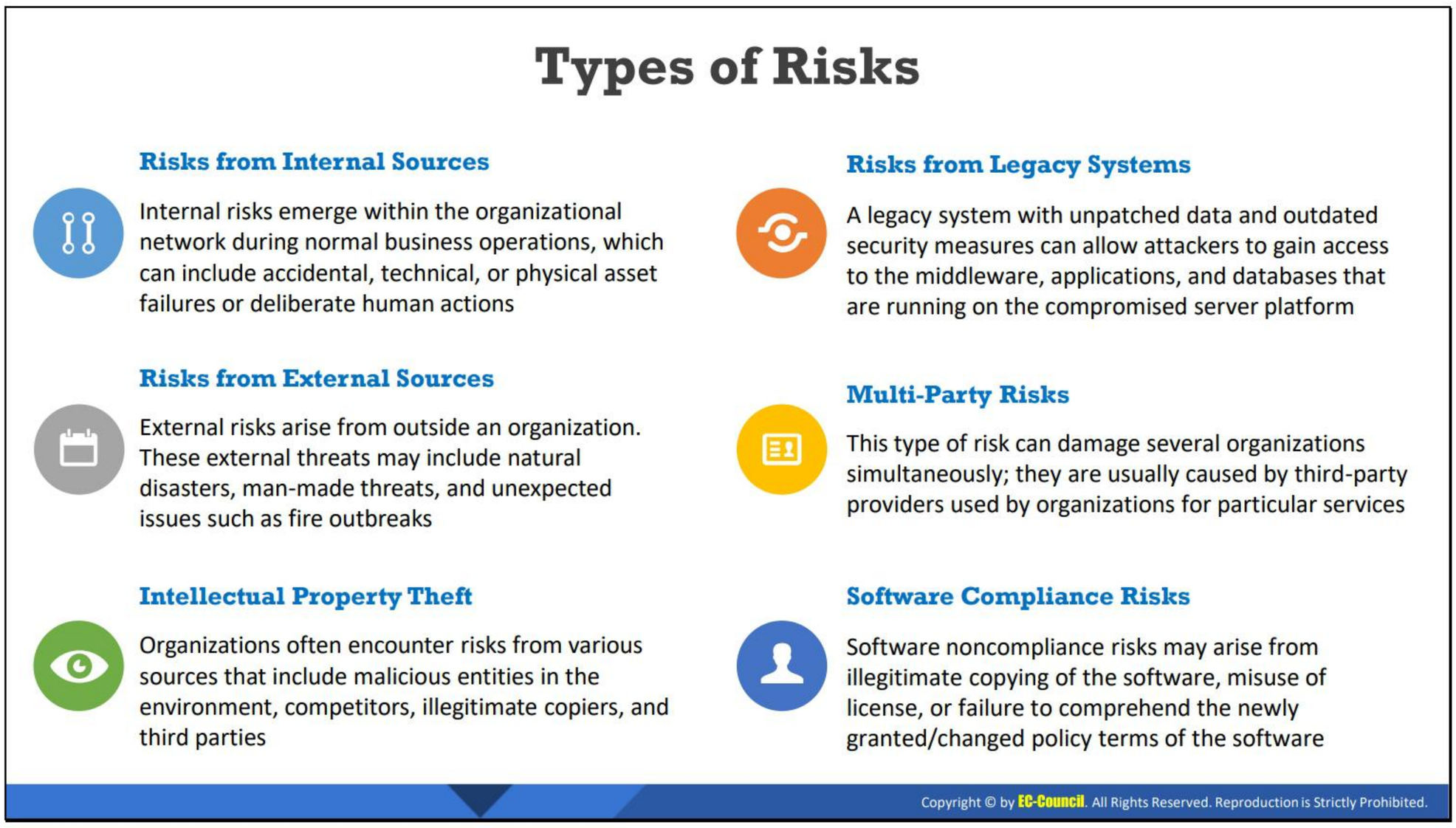
Features of Effective KRIs

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

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

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

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



Types of Risks

Risk is the likelihood of the occurrence of an event that can adversely impact the systems or processes running in an organization. A risk is defined as a significant damage or loss due to exposure to vulnerabilities or misuse of technology and technical assets. These risks can be extended beyond the damage and destruction of data; they can cause significant loss in business and damage the reputation. The types of risks may vary for each organization.

Various types of risks are discussed below:

- **Risks from Internal Sources**

  Internal risks emerge within the organizational network during normal business operations, which can include accidental, technical, or physical asset failure or deliberate human actions. They can be predicted in advance and mitigated by taking necessary actions. However, it is difficult to identify these risks occasionally, especially when they are caused by disgruntled employees; in such cases, it is mandatory to verify whether a risk is caused by malicious intention or accidental outbreak.

  An employee of an organization can be responsible for the breach of confidential organizational data, intentionally or unintentionally, depending on their internet usage. This encourages external attackers to penetrate the target system and cause more damage to the organizational data.

- **Risks from External Sources**

  External risks arise from outside an organization. These external threats may include natural disasters, man-made threats, and unexpected issues such as fire outbreaks. A malicious user or attacker who gains access to an organizational system or server by exploiting the existing vulnerabilities or bugs can perform attacks such as malware

injection from remote systems, manipulating the services, and stealing confidential information to disrupt operations, which can eventually lead to loss of productivity.

Sometimes, attackers can also hide their presence on compromised systems for numerous days. In such cases, it becomes difficult for authorized users or organizations to identify their presence until the damage occurs.

- **Intellectual Property Theft**

  Intellectual property theft is the process of stealing the idea of an organization or individual by an entity and promoting it as their property. Intellectual property is a type of property that is created by human intelligence and it is legally protected and owned by an organization or individual. These properties include business secrets, authorized signatures, copyrights, and patents. Organizations often face risks from various sources including malicious entities in the environment, competitors, illegitimate copiers, and third parties.

  Intellectual property theft in a smaller organization or start-ups can cause significant damage in terms of economy, business growth, and competitive withstand. To protect businesses and assets in the long term, product owners must have proper knowledge about the techniques implemented by intellectual property theft actors.

- **Risks from Legacy Systems**

  A legacy system is a computing device or software running an outdated version. Because they do not receive any patches or updates, they can cause potential harm to the organizational network.

  These systems can be incompatible with the upgraded technology, lack security support, have high maintenance costs, and involve complicated modification and patching techniques. However, some legacy systems are still in use for specific purposes. Sometimes, installing critical updates on legacy systems may invite several risks because they can break the system functionalities.

  Although upgraded services and capabilities such as data integration and cloud computing are widely deployed in the market, most of the small and moderate businesses that use legacy systems do not have proper modern data disaster recovery, backup, and other security-related services. Such organizations might face various risks that can destroy their businesses.

  A legacy system with unpatched data and outdated security measures can also enable attackers to obtain access to the middleware, applications, and databases that run on the compromised server platform.

- **Multi-Party Risks**

  This type of risk can damage several organizations simultaneously. They are usually caused by third-party providers that organizations rely on for particular services. If an event occurs at the provider end, it can impact the organizational business or risk the organizational data. To address these issues, multiparty computation or secure

multiparty computation can be employed, which is a cryptographic primitive that shares the computational process over the network of several parties and maintains data privacy by restricting one party to view the data related to other parties. It performs joint analysis on the data of an individual without exposing their data to other individuals.

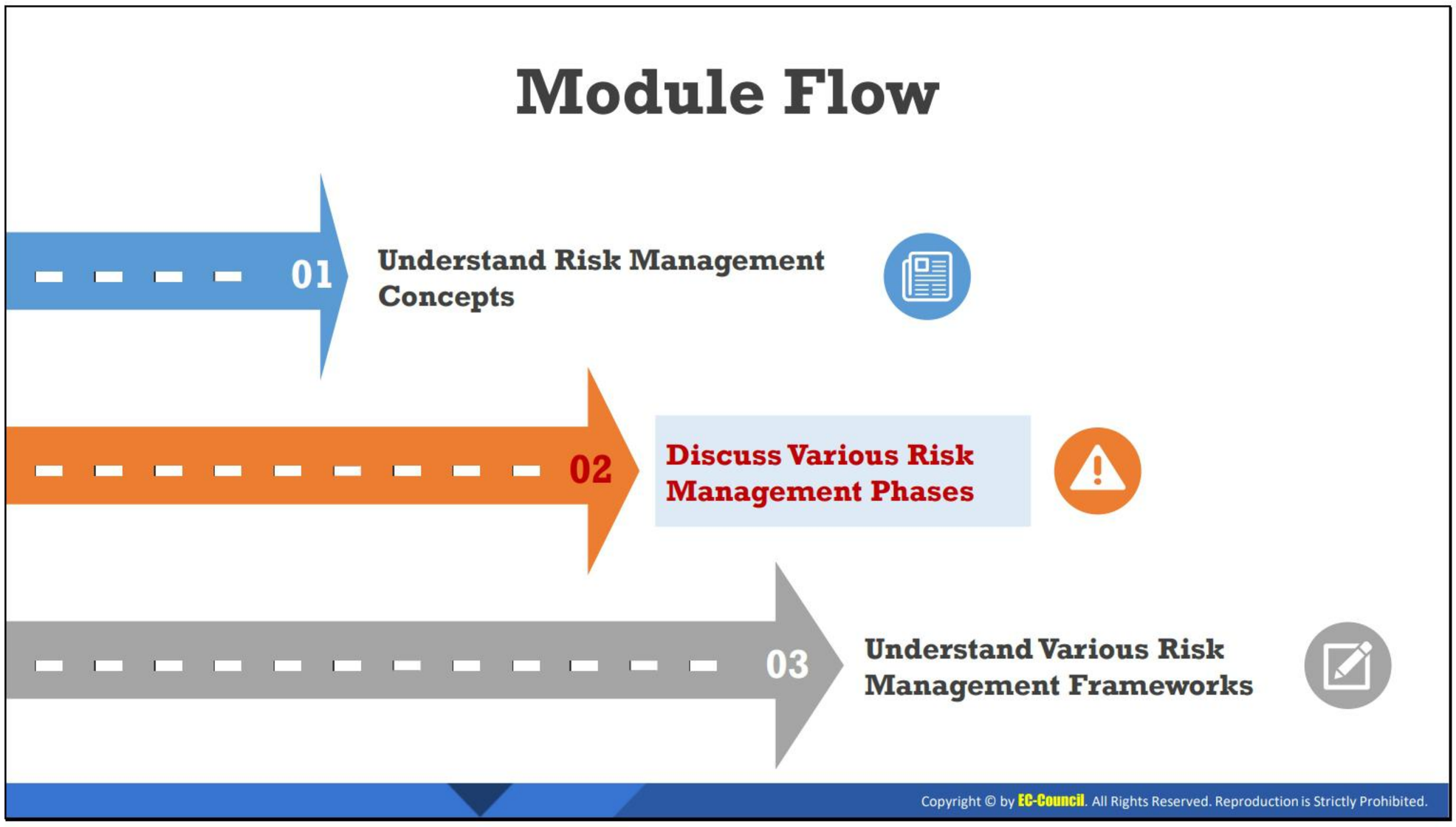
- **Software Compliance Risks**

  The word compliance in software defines a state of following the guidelines or standards while developing or installing an application or software. Organizations are provided with a publisher licensing contract or agreement when an application or software is deployed at their end.

  Software noncompliance risks may arise from the illegitimate copying of the software, inadequate asset management systems, misuse of license, inefficient software audits, failure to keep the contract record, over budgeting for server licensing, under budgeting for client licenses, and failure to comprehend the newly granted/changed policy terms of the software. Therefore, network administrators must be trained considering appropriate terms and conditions to install specific applications or software along with the legal risks associated with them.

  The risks associated with software compliances are discussed below:

  - **Legal Risk:** It represents non-compliance to the software license agreement and inability to meet the corporate standard requirements.
  - **Operational Risk**: It represents the inadequate and inappropriate usage of licenses that leads to poor business decision-making.
  - **Financial Risk**: It represents the over expenditure, inaccurate budgeting, and undisclosed liabilities on software licenses.



Discuss Various Risk Management Phases

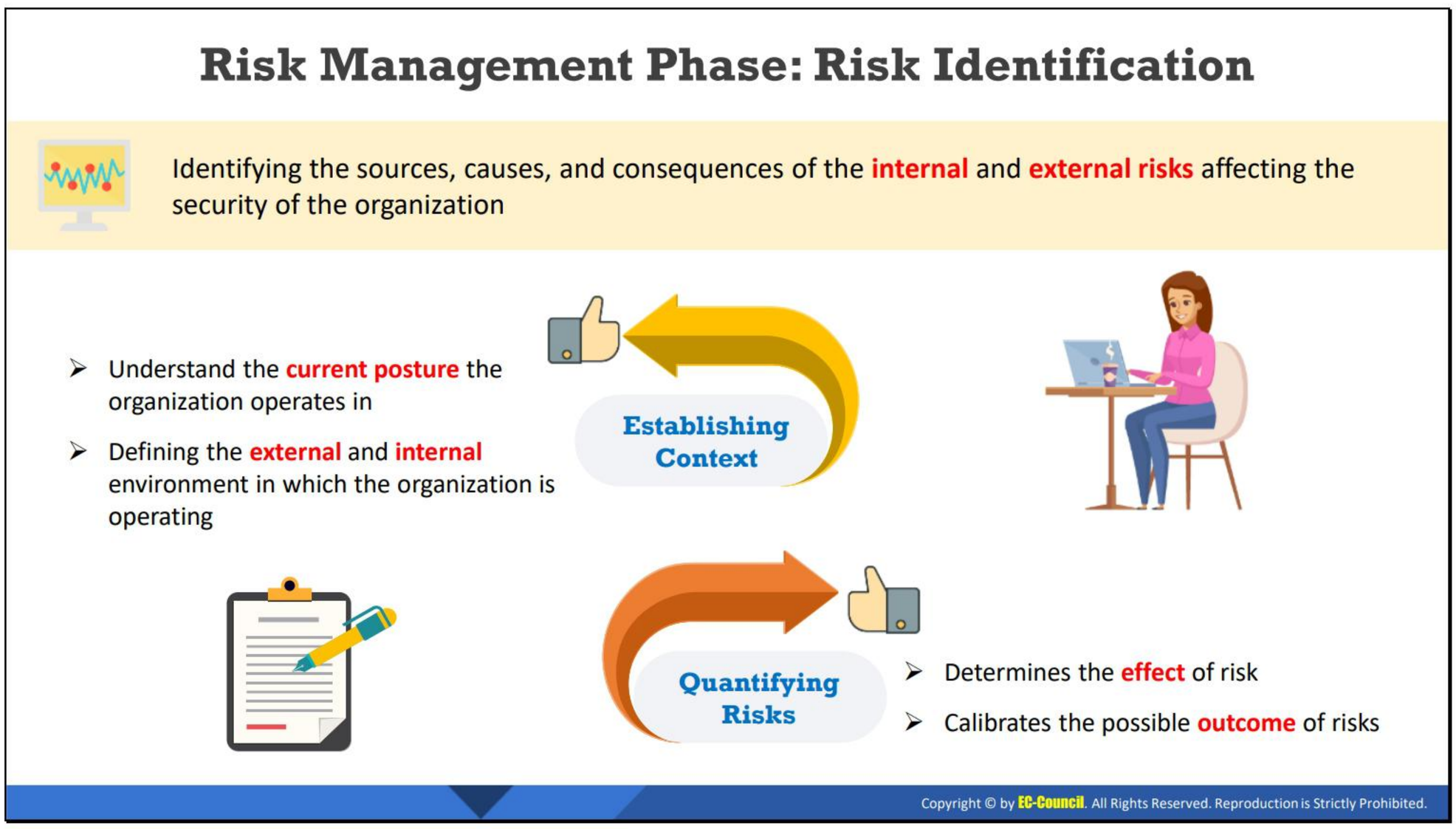
This section explains risk management phases involved in an organization's risk management program.

Risk Management Phases

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

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

1. Risk identification
2. Risk assessment
3. Risk analysis
4. Risk prioritization
5. Risk treatment
6. Risk tracking and review



Risk Management Phase: Risk Identification

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

Role of Risk Identification

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

Risk Identification Steps

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

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

Main Elements in Risk Identification

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

Priorities of Risk Identification

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

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

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

Document the risks, which includes:

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

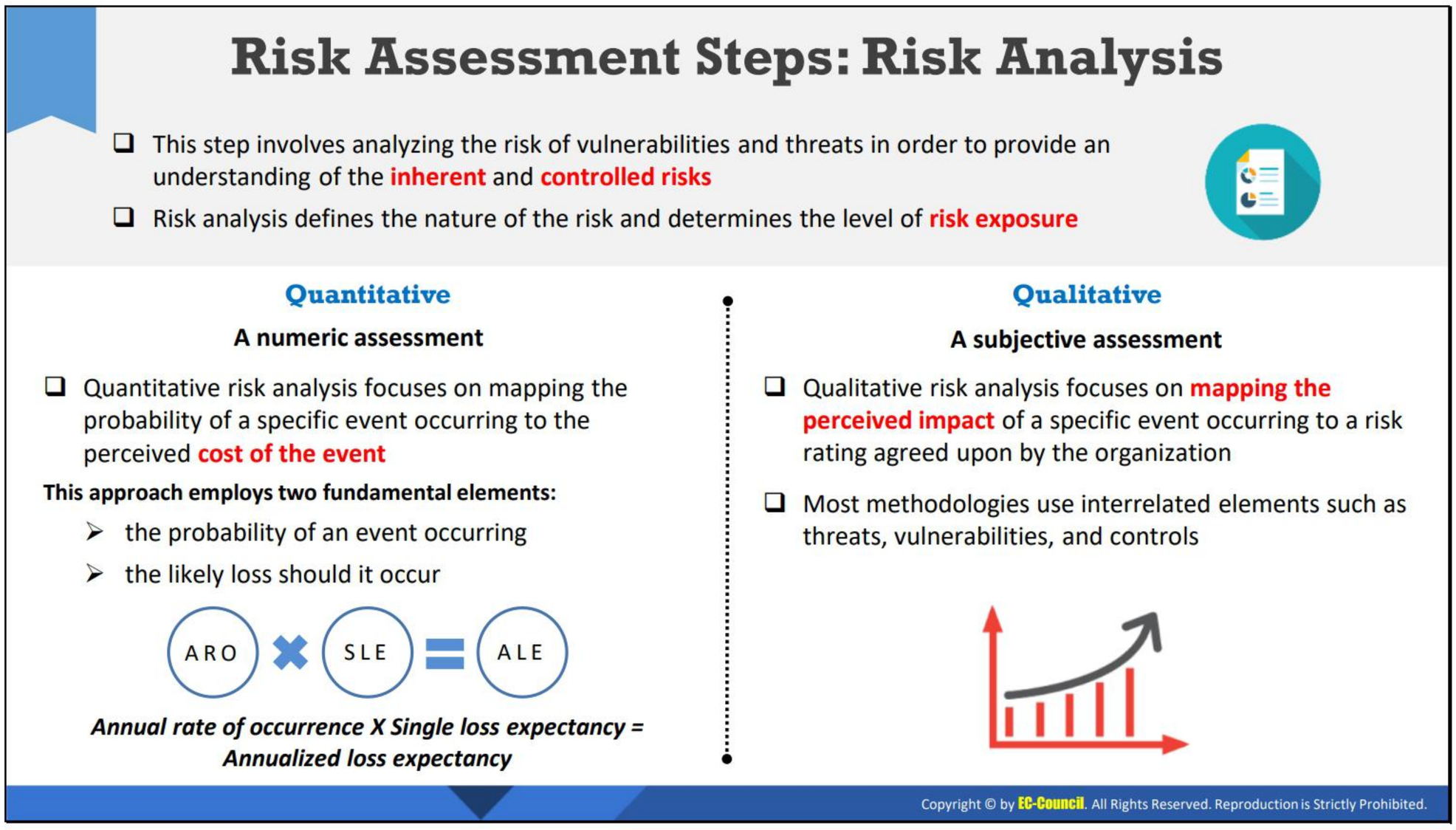
Risk Management Phase: Risk Assessment

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

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

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

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



Risk Assessment Steps: Risk Analysis

This step involves analyzing the risk of vulnerabilities and threats in order to provide an understanding of the inherent and controlled risks. Risk analysis defines the nature of the risk and determines the level of risk exposure.

Information security risk assessment begins by selecting an approach to evaluate the risks encountered by an organization. The two most common approaches for risk analysis include quantitative risk analysis and qualitative risk analysis.

- **Quantitative Risk Analysis**

  Quantitative risk analysis focuses on mapping the probability of occurrence for a specific event to the expected cost associated with the event. This analysis is represented as a standard formula in which the annualized rate of occurrence (ARO) is multiplied by the single loss expectancy (SLE) to produce the annualized loss expectancy (ALE).

  ARO x SLE = ALE

- **Qualitative Risk Analysis**

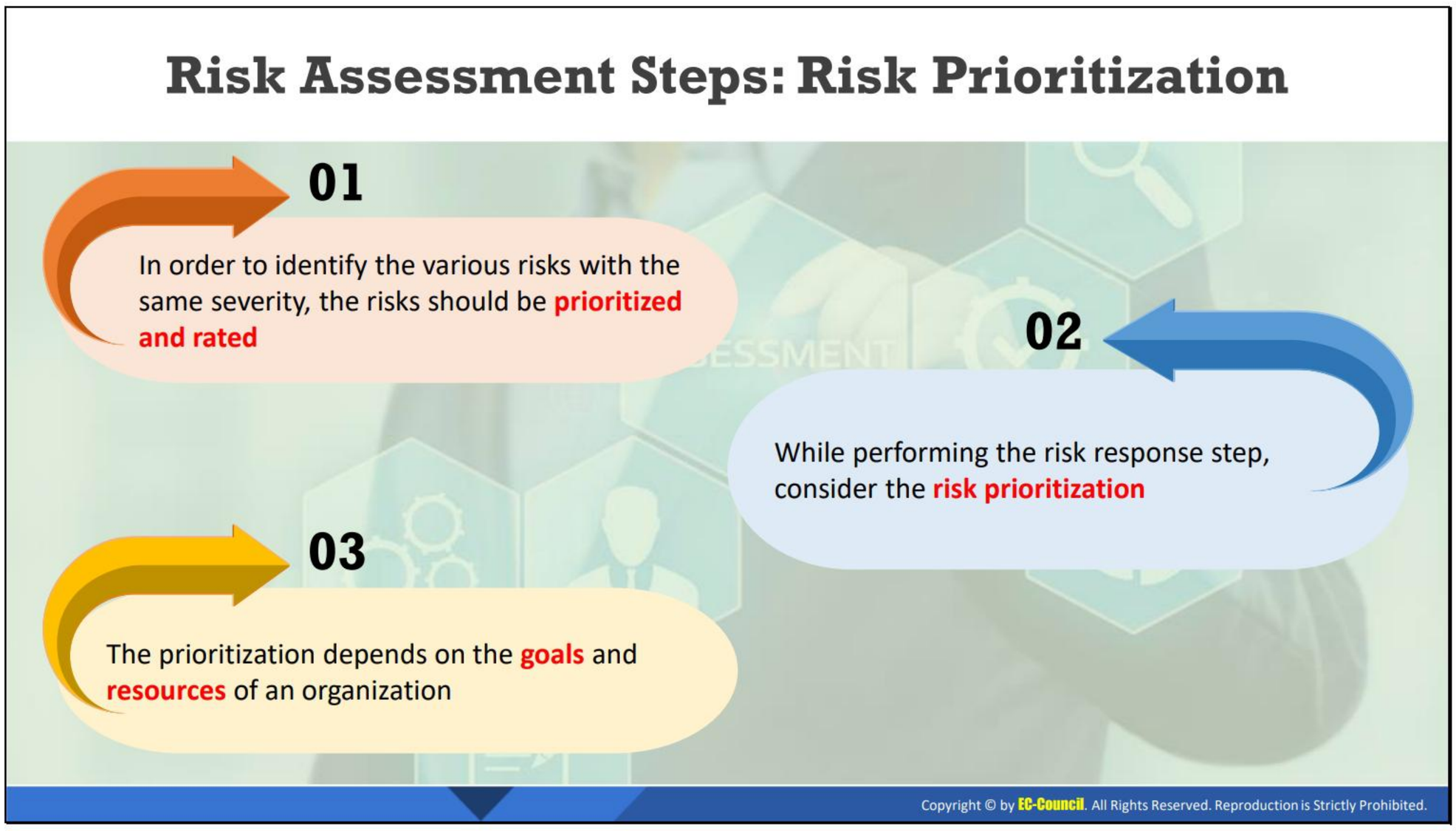
  Qualitative risk analysis focuses on mapping the perceived impact of a specific event occurring to a risk rating agreed upon by the organization. This subjective analysis approach is less precise than the quantitative approach; however, probability data and mathematical formulas are not required to estimate information security risks.

  Most qualitative analysis approaches combine interrelated elements like threat information, vulnerabilities, and control information to support an assessment based on impact. This allows the flexibility to define risk according to categories like low,

moderate, and high (or red, yellow, and green) to facilitate conversations about risk in terms that are understood by most people.

ISO 27005 suggests that qualitative risk analysis is appropriate in the following situations:

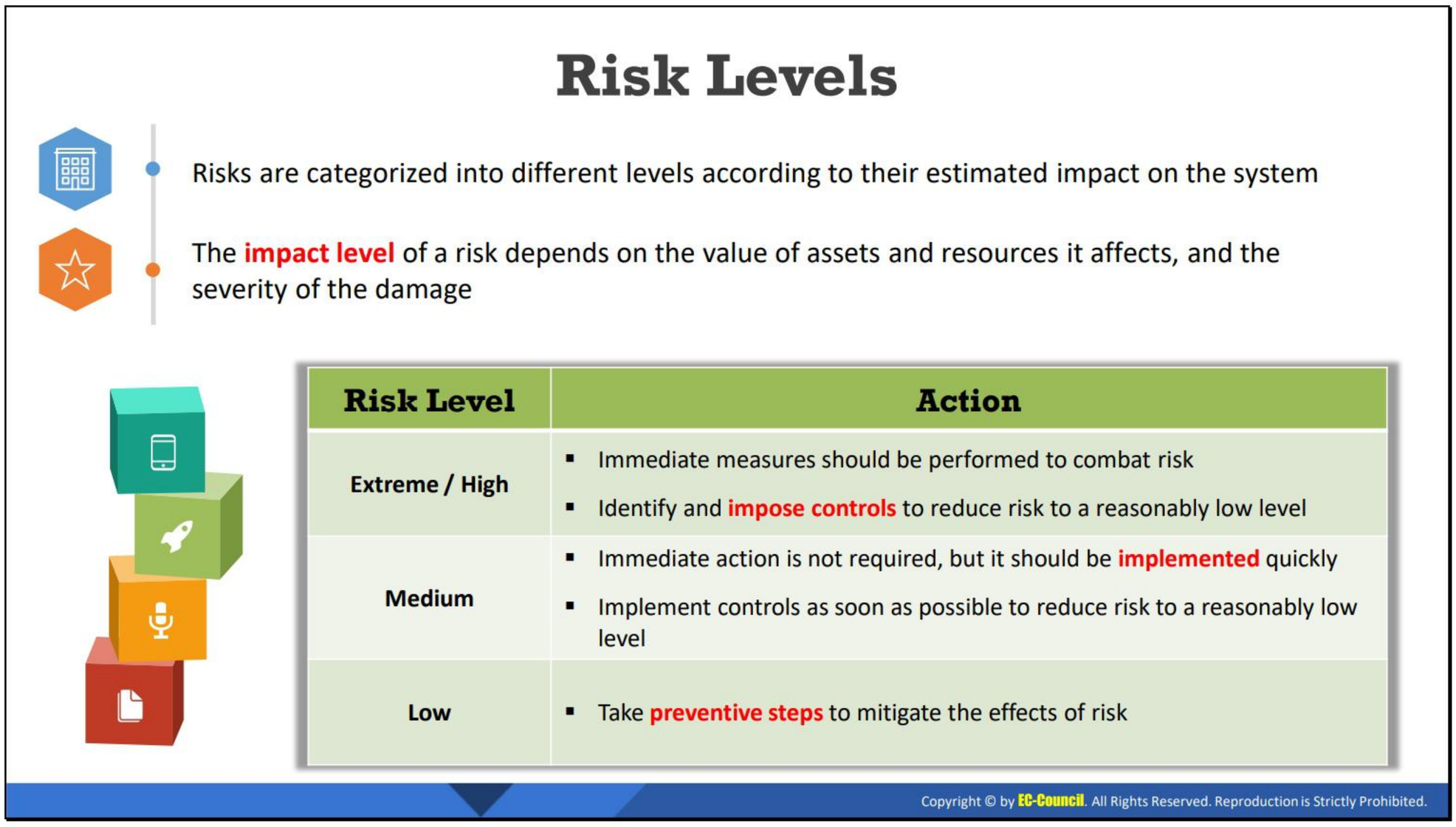
- As an initial screening activity to identify risks that require more detailed analysis
- Where this kind of analysis is appropriate for decisions
- Where the numerical data or resources are inadequate for a quantitative risk analysis



Risk Assessment Steps: Risk Prioritization

In order to identify the various risks with the same severity, the risks should be prioritized and rated. This way, an appropriate response plan may be designed. The prioritization depends on the goals and resources of an organization. Consider the following for risk prioritization:

- Immediate and future impact of a risk on an organization's goals, assets, other organizations, and the nation in order to prioritize risks
- Expected loss because of a risk
- Relationship of a risk and/or mitigation to other risks and/or mitigations
- Managing the impact of threats from a risk

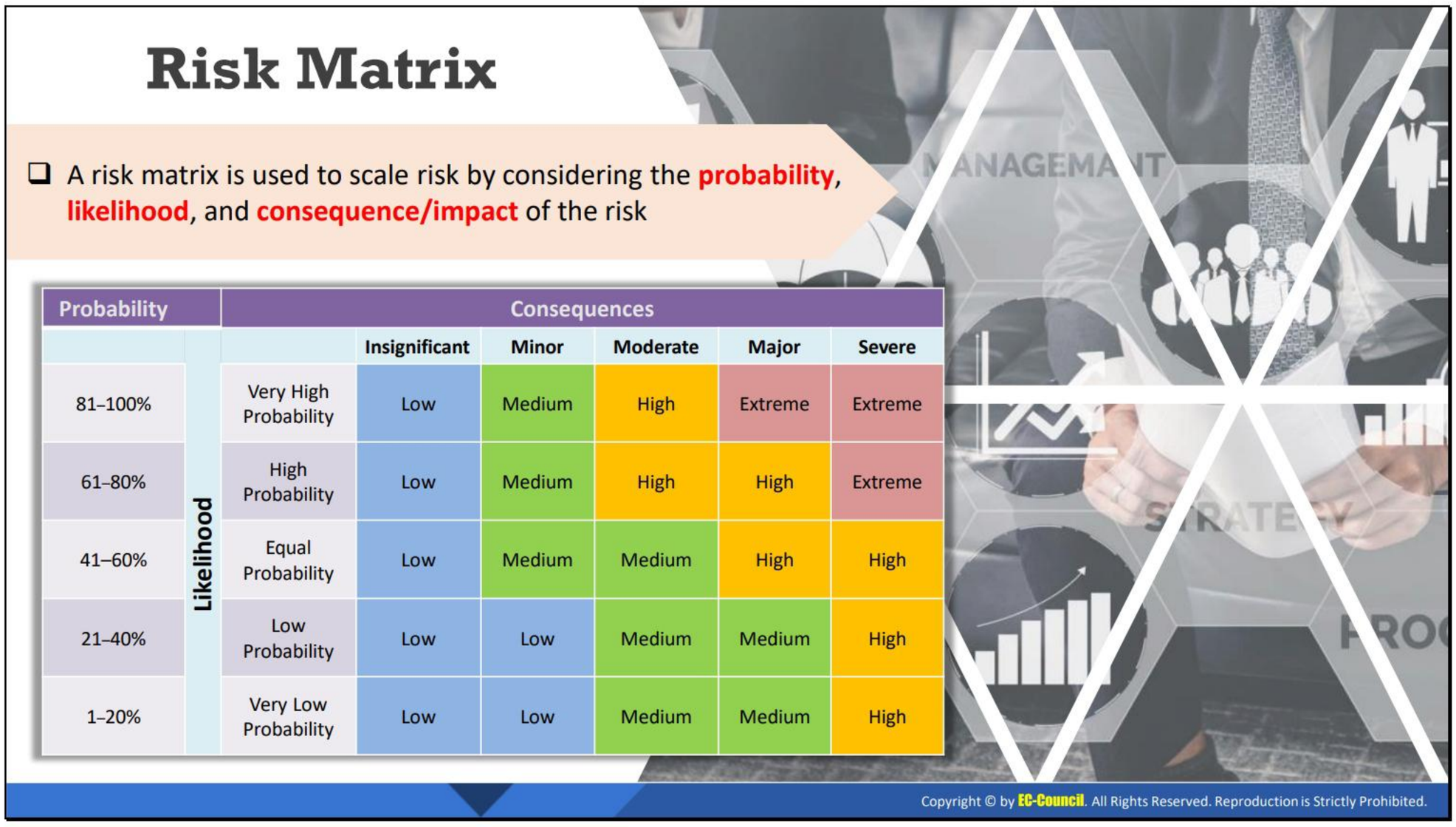


Risk Levels

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

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

Table 22.1: Risk levels and action



Risk Matrix

A risk matrix is used to scale risk by considering the probability, likelihood, and consequence/impact of the risk. The risk assessment matrix is a useful tool to identify the probability of failure and high-risk areas. In addition to risk levels, a risk-level matrix needs to be developed to measure or assess a risk.

Here,

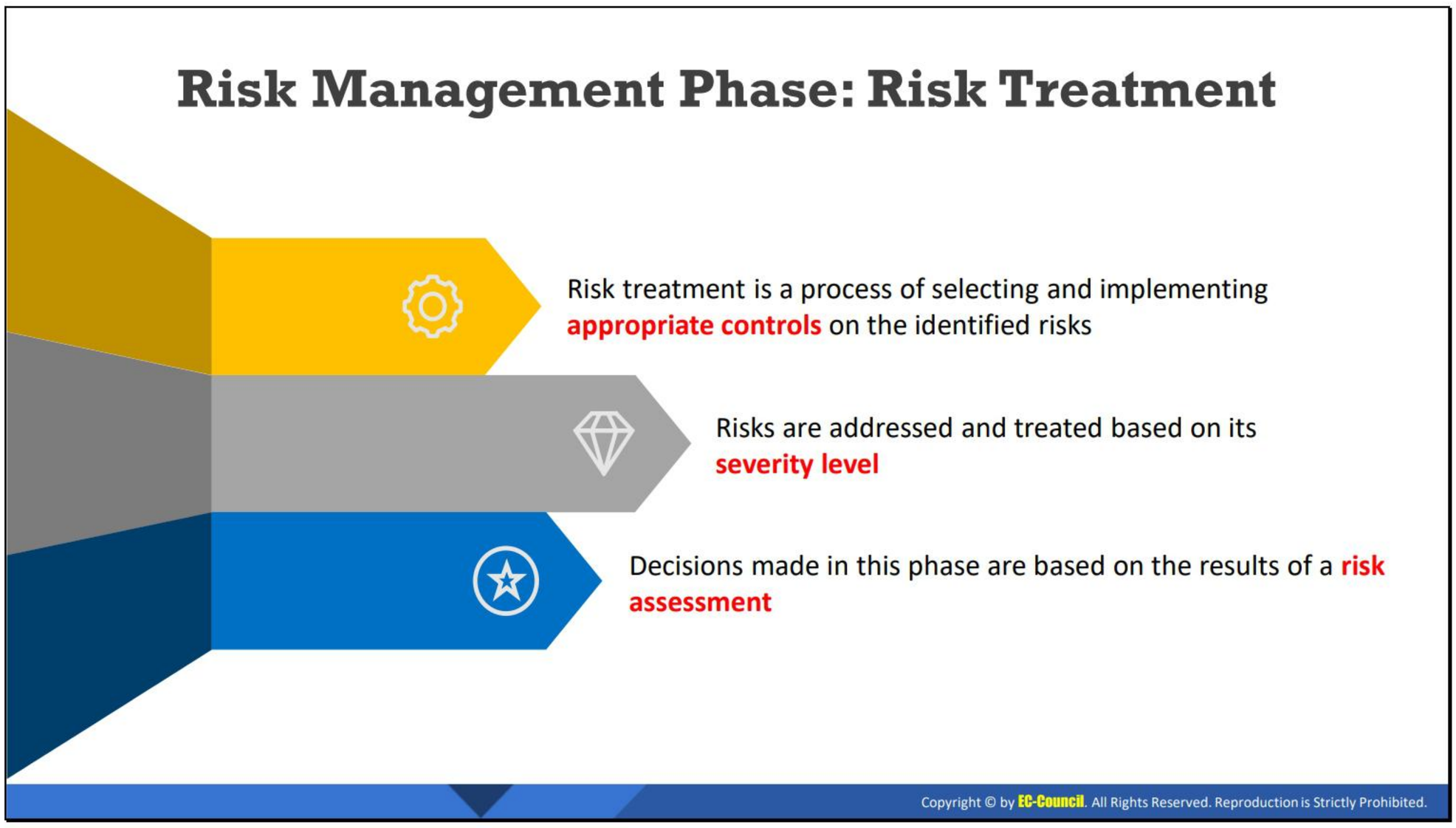
`Risk rating = Probability(Likelihood) x Severity,`

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

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

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 22.2: Risk matrix



Risk Management Phase: Risk Treatment

Risk treatment is the process of selecting and implementing appropriate controls on the identified risks in order to modify them. The risk treatment method addresses and treats the risks according to the risks' severity level. Some of these measures are discussed below.

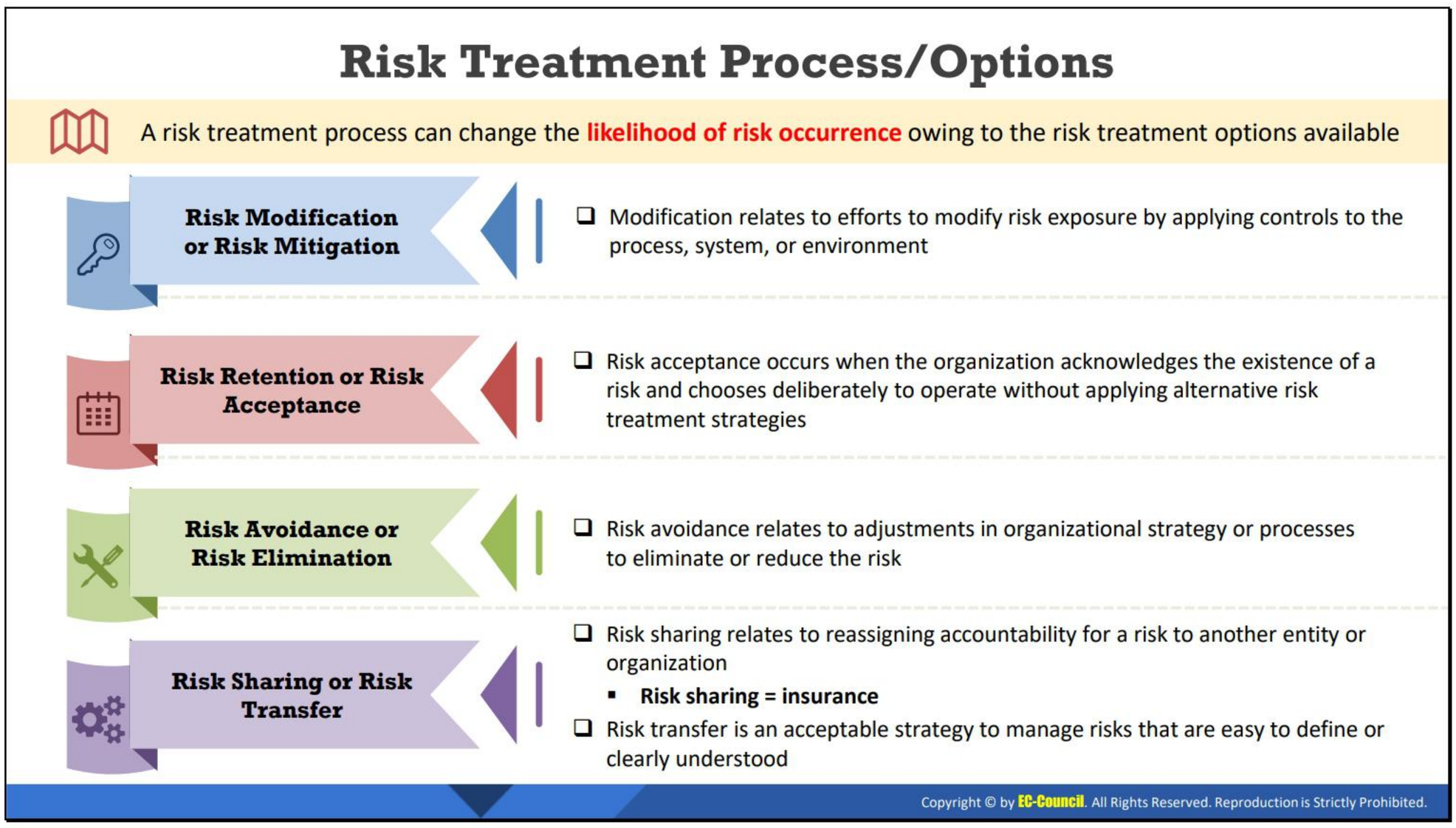
Decisions made in this phase are based on the results of a risk assessment. This step identifies treatments for risks that fall outside the department's risk tolerance and provide an understanding of the level of risk along with controls and treatments. It identifies the priority order in which individual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

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

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

Actions to Minimize or Eliminate Risk

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



Risk Treatment Process/Options

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

Risk Treatment Options

- **Risk Modification or Risk Mitigation**

  Risk modification is the most common risk treatment option. An organization seeks to change risk exposures or outcomes by applying security controls to a process, system, or environment when they are performing risk modification. Some risk management frameworks describe modification in terms of mitigation—the extent to which the severity of the risk has been reduced. Because modification is commonly associated with the application of security controls, it is important that the security professional understanding the types of controls available and the objectives of those controls.

- **Risk Retention or Risk Acceptance**

  Risk acceptance often occurs when an organization acknowledges the existence of a risk and chooses deliberately to operate without applying one of the other treatment options available. The organization accepts the potential outcome of the identified risk while understanding the potential impact to the organization. Some level of risk always exists, even after applying controls to support mitigation. Risk acceptance in these cases applies to the residual risk that remains.

  Risk acceptance often maps to the organization's perceptions or feelings about risk. The security professional must communicate the risks and potential outcomes that exist, but the organization has the responsibility to choose whether or not to accept risk as a

treatment strategy. Organizations should define policies and procedures for risk acceptance as part of corporate governance. Optimally, the policies and procedures should define requirements for escalation and approval of risk acceptance to ensure accountability for the decision.

- **Risk Avoidance or Risk Elimination**

  Avoidance is a risk treatment option that occurs when an organization makes changes or avoids an activity to remove risk and eliminate its effect on the activity altogether. For example, an organization may choose not to build a new facility because of the outcome of a risk assessment. Instead of applying controls to address natural disasters or other physical threats, the organization chooses to build in another location to eliminate the identified risk.

- **Risk Sharing or Risk Transfer**

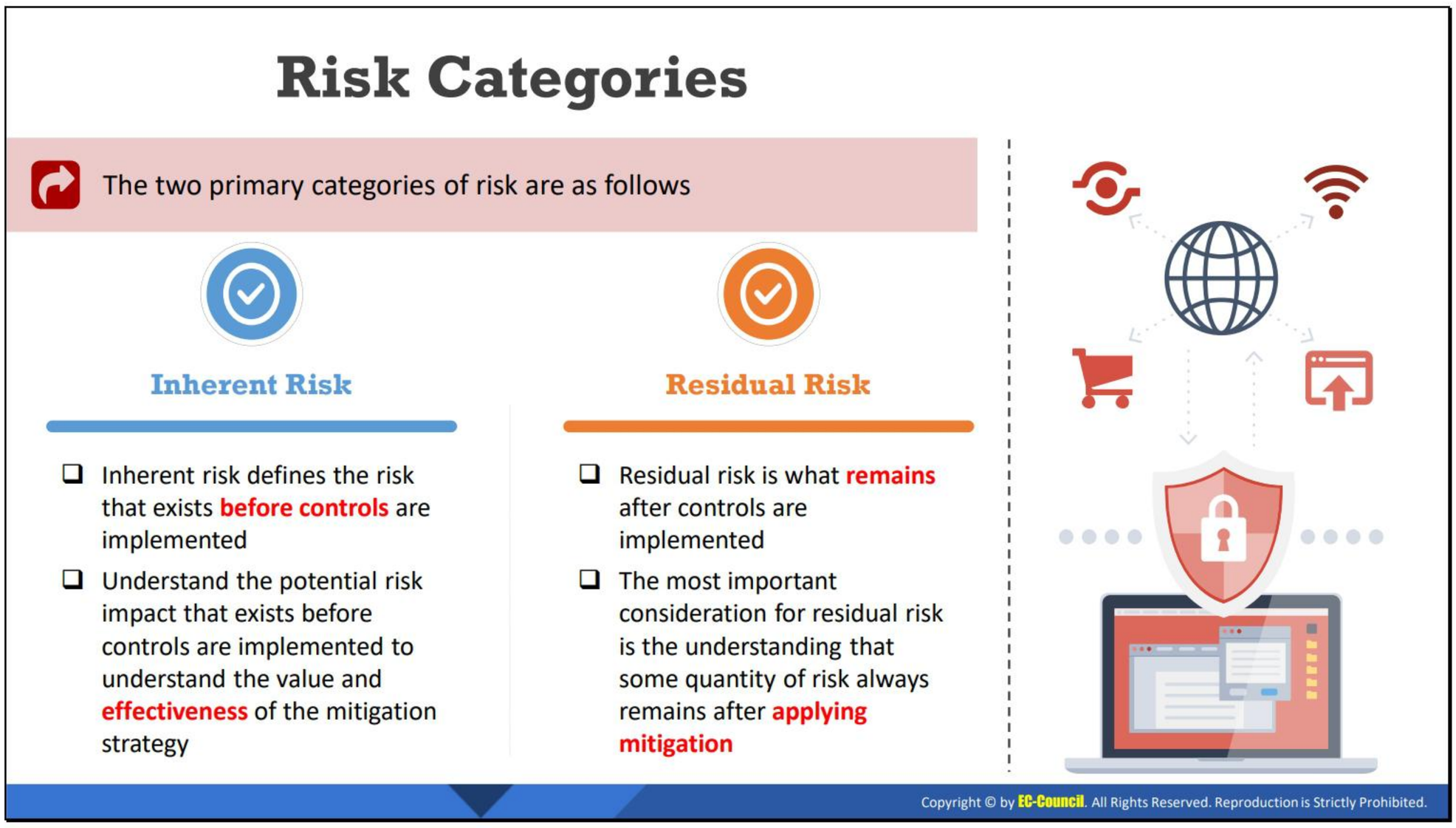
  Risk sharing relates to reassigning accountability for a risk to another entity or organization. Most often, this is accomplished by purchasing insurance that will reduce the direct costs of a covered event or reduce the cost of remediation. This risk treatment option also applies to distribution of risk between business partners. Although shared or transferred risk can reduce costs associated with risk management, an organization cannot transfer risk entirely to another organization. The organization ultimately owns the risk, and shares the cost of potential outcomes.

  Risk transfer is an acceptable strategy to manage risks that are easy to define or clearly understood. Risks that are difficult to quantify may increase the risk profile because a loss of influence or control is assumed when an organization transfers or shares risk with another entity. For example, cyber insurance may cover a data breach, but the policy only pays if specific criteria are met for an event with a root cause and outcome that varies widely from one organization to the next.

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

- Implement an appropriate risk treatment option
- Ensure adequate resources are available while implementing the risk treatment plan
- The risk treatment plan should reduce the risk factor to a certain acceptable level
- Remedial actions should be taken for risks that need to be handled immediately

Note: The risk treatment options do not always mitigate risks completely. Often, residual risks persist, and these need to be considered as well.



Risk Categories

The two primary categories of risk are as follows:

- **Inherent Risk**

  Inherent risk defines the risk that exists before controls are implemented. The organization must understand the potential risk impact that exists before controls are implemented to understand the value and effectiveness of the mitigation strategy.

- **Residual Risk**

  The idea that some quantity of risk remains after controls are applied is the most important idea about residual risk. Risk mitigation exists to reduce risk to an acceptable level, but that level is rarely zero unless the organization chooses avoidance as the risk treatment strategy. Risk acceptance, therefore, applies as a normal outcome of reducing risk to the lowest acceptable residual level.

Risk Treatment Plan

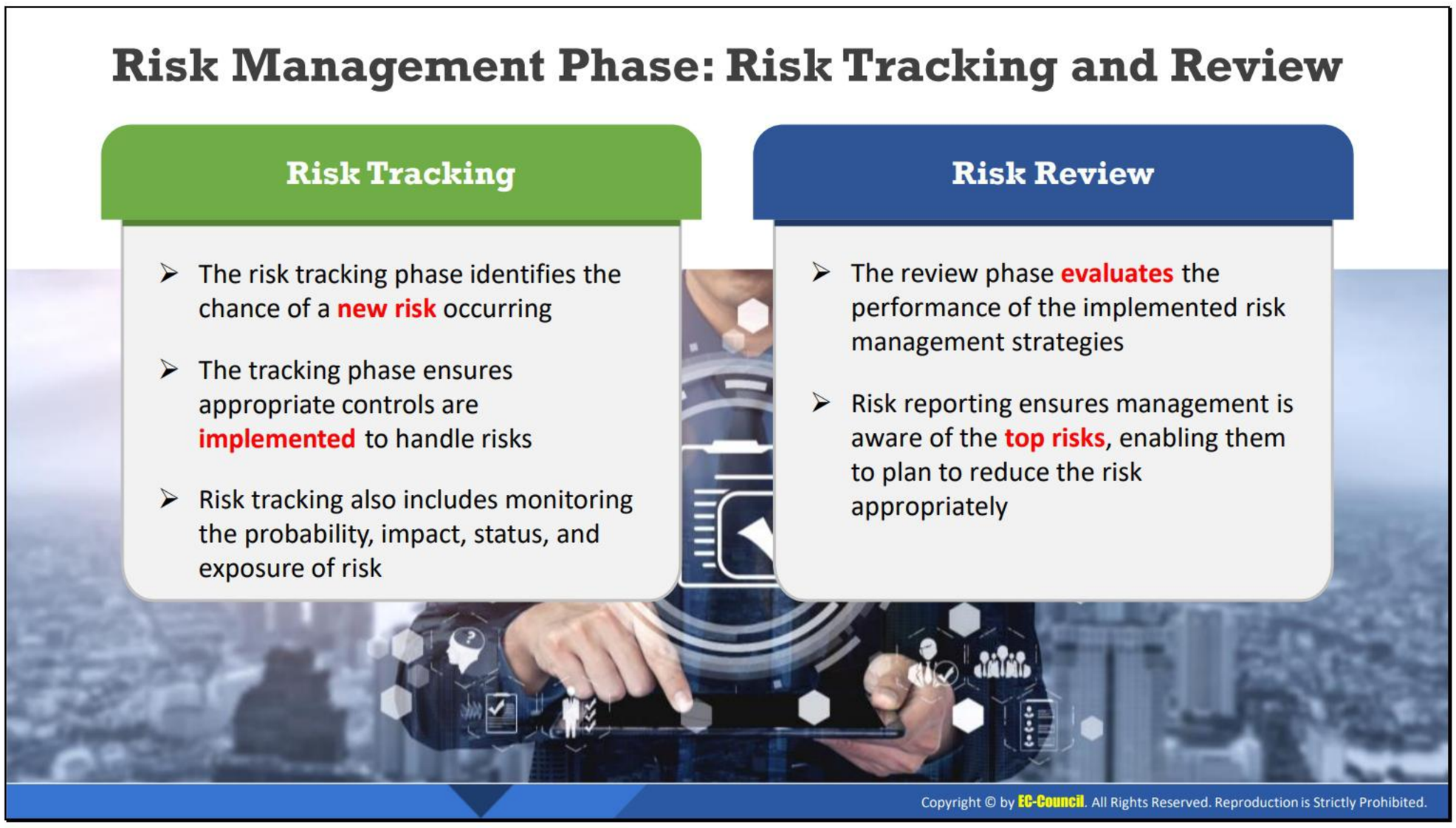
The risk treatment plan is the action plan that describes the plan to respond to potential risks. It provides a summary of the identified risks, every risk's designed response, parties responsible for all risks, and target date for risk treatment. It is one of the essential documents an organization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

Steps for Risk Treatment Plan

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

To ensure risk treatment plans are implemented corrected and monitored accurately, the security professionals needs to ensure

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



Risk Management Phase: Risk Tracking and Review

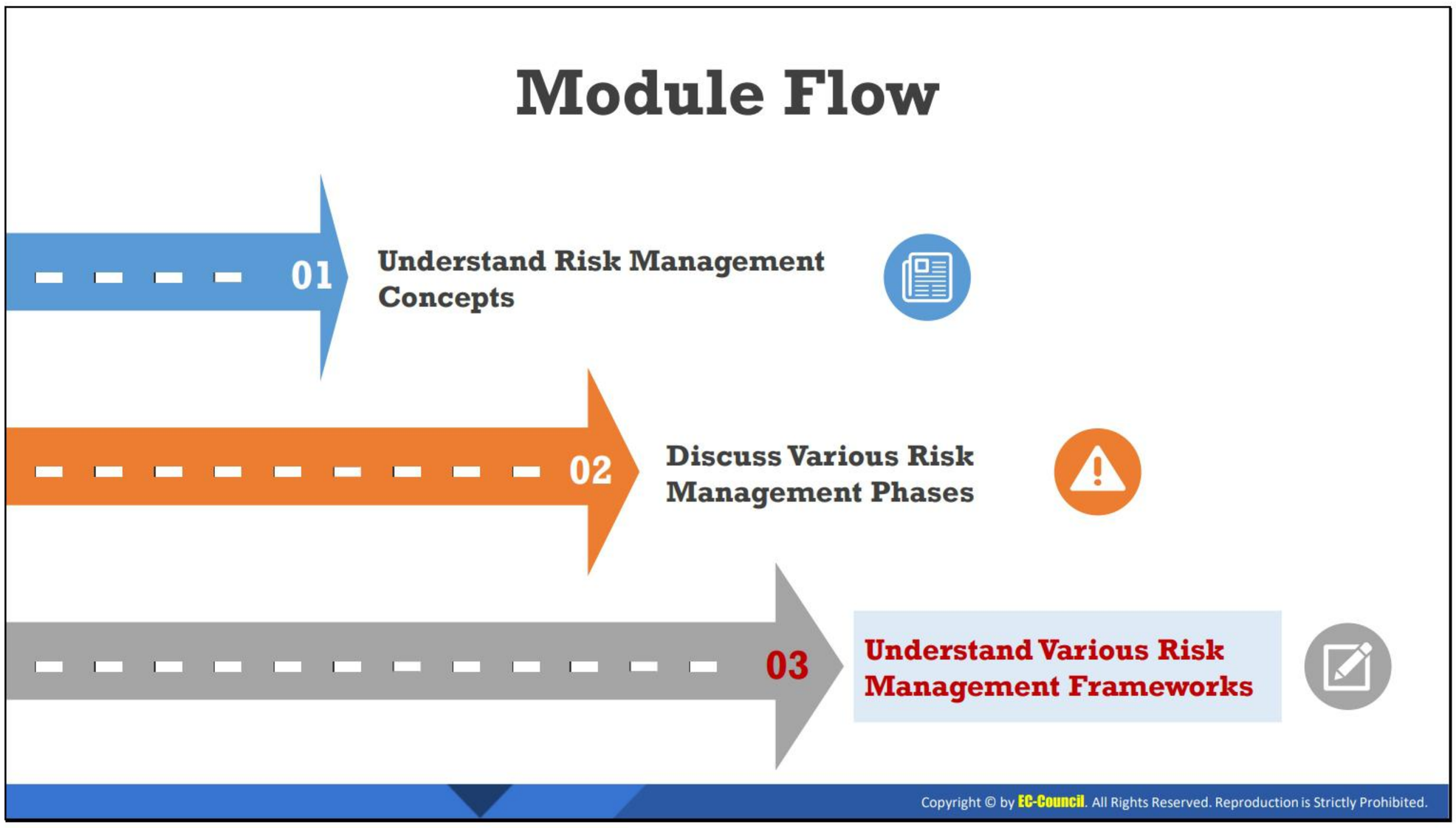
For the risk management process, well-planned and regular monitoring and review are required in order to identify new risks and reduce them appropriately.

- **Risk Tracking**

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

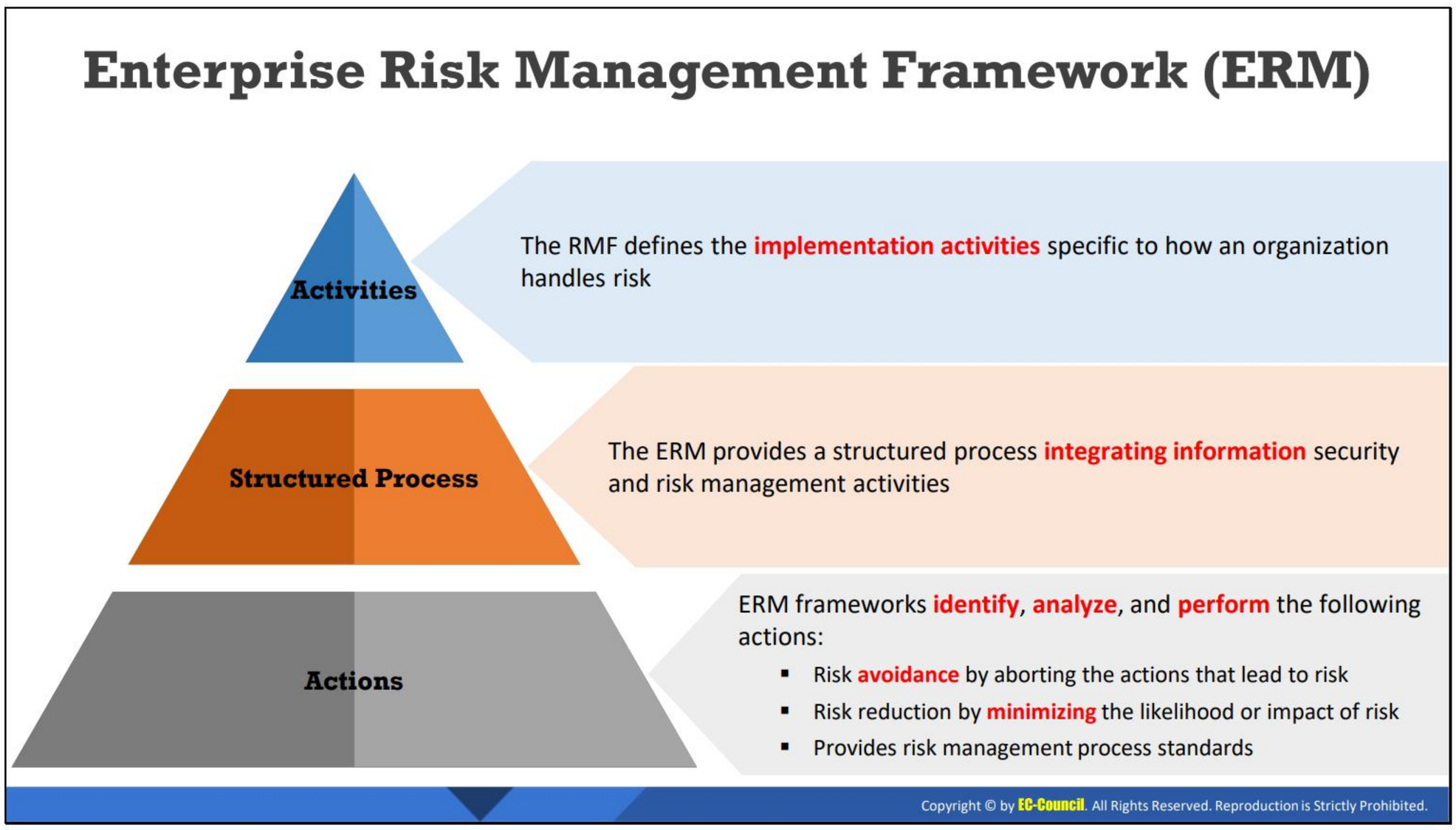
- **Risk Review**

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



Understand Various Risk Management Frameworks

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



Enterprise Risk Management Framework (ERM)

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

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

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

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

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

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

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

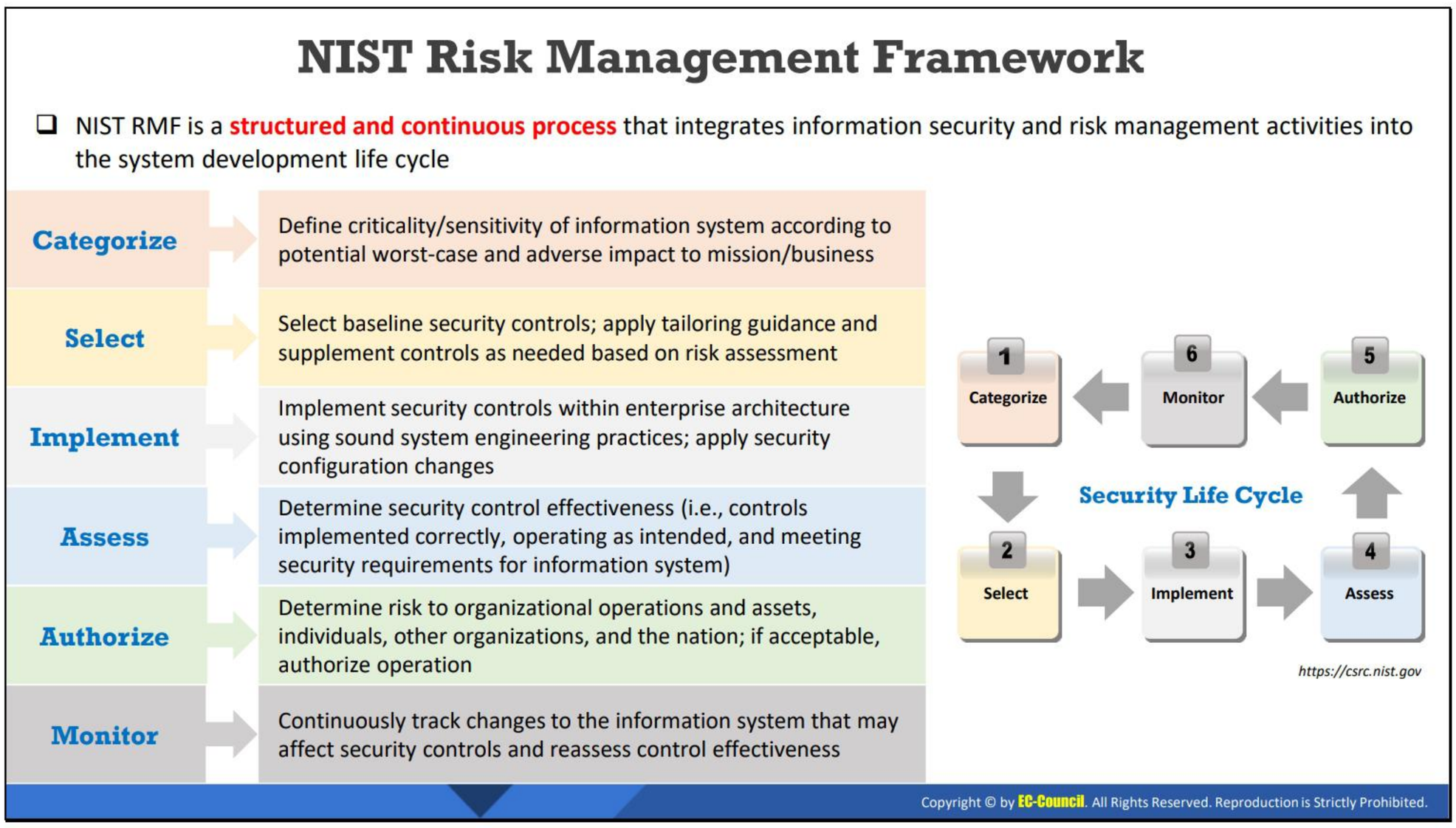
This ERM framework helps an organization understand the following:

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

Goals of the ERM Framework

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

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



NIST Risk Management Framework

Source: *https://csrc.nist.gov*

The National Institute of Standards and Technology (NIST) RMF is a set of information security policies and standards for the federal government developed by NIST. It is a structured and continuous risk management process that is integrated into a system development life cycle. The RMF process helps early detection and resolution of risks.

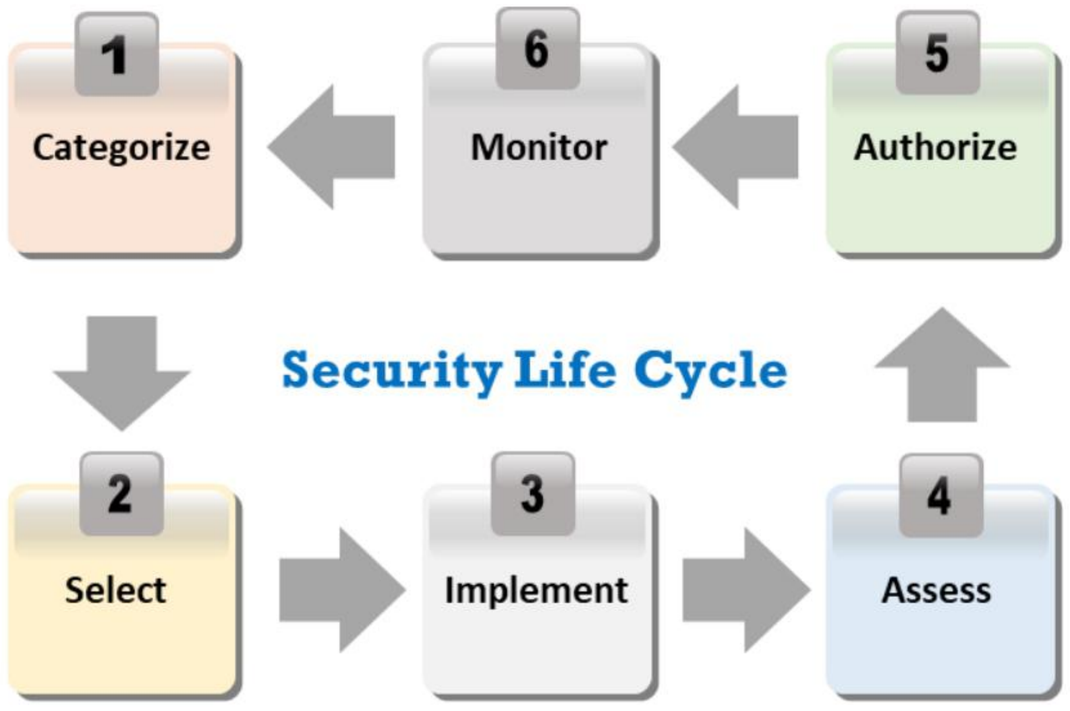
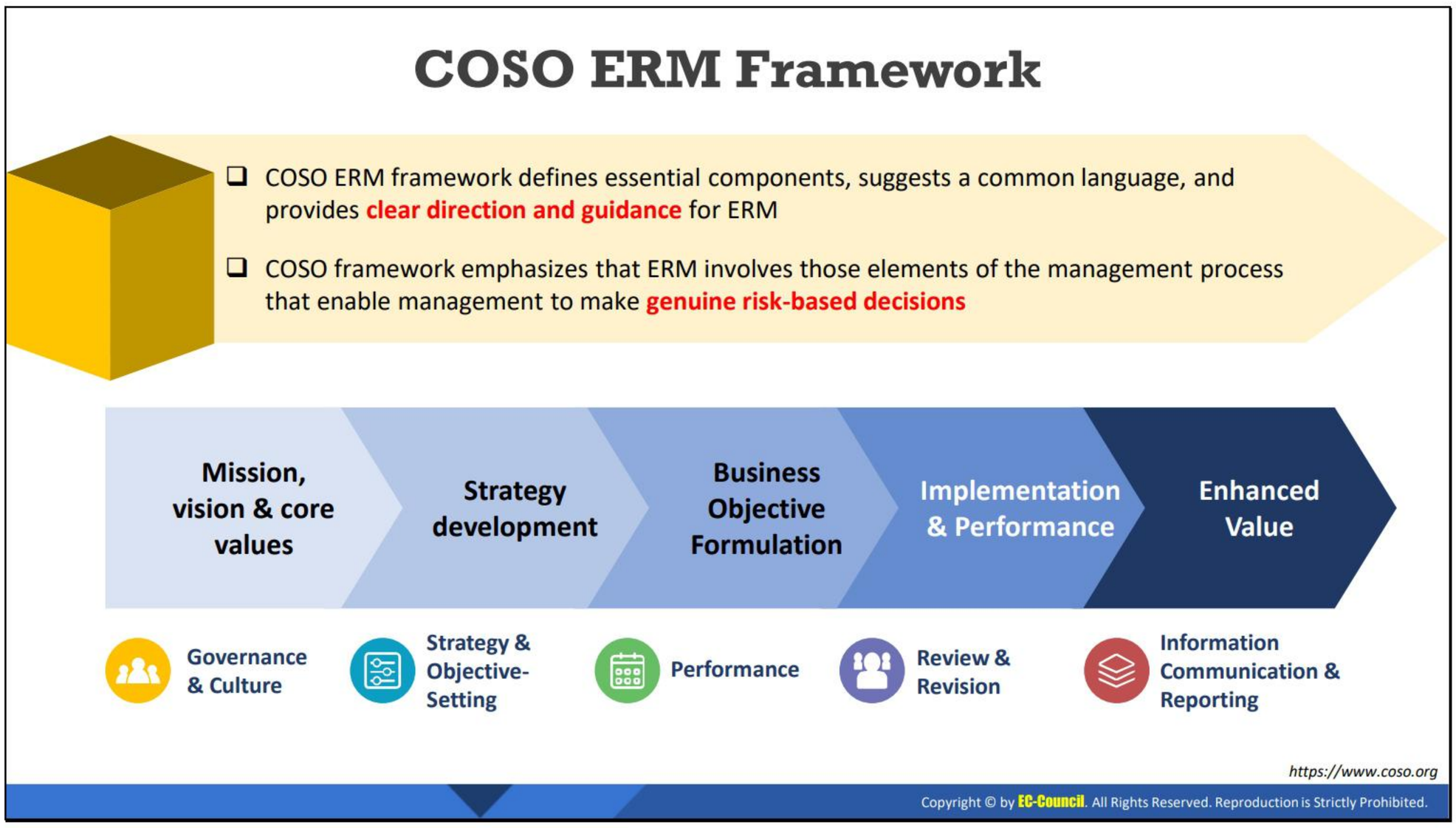


Figure 22.1: NIST RMF security system lifecycle

It identifies the following processes (tasks) for managing organizational risk, which can be applied to both new and legacy systems:

- **Categorize:** Categorize the information system and the information processed, stored, and transmitted by a system according to potential worst cases, adverse impact to an organizations mission/business functions, and a system.

- **Select:** Select the appropriate baseline security controls based on the categorization in the first step, and implement security controls based on the risk assessment.
- **Implement:** Implement security controls and integrate security controls with legacy systems using sound system engineering practices; then apply security configuration settings and document the implemented security controls and their impact on the environment.
- **Assess:** Evaluate the implemented security controls for effectiveness using appropriate procedures and determine if the controls implemented are working correctly and effectively; check if they are producing the desired outcome with respect to meeting the security requirements for a system.
    - **Steps in Assessment**
        - Develop the security assessment plan
        - Determine which controls are to be assessed
        - Select appropriate procedures to assess those controls
        - Determine depth and coverage needed for assurance
        - Tailor the assessment procedures
        - Finalize the plan and obtain approval
        - Conduct the assessment
        - Analyze the results
        - Create the security assessment report
- **Authorize**: Determine the risks to organizational operations and assets, individuals, other organizations, and the nation based on the accepted risk appetite with respect to operations and assets (how much risk an organization is willing to tolerate) if acceptable; then, authorize the operation or decide on the required needs.
- **Monitor:** Continuously track changes to the information system for signs of attacks that may impact security controls, and regularly monitor the security controls to access their effectiveness.



COSO ERM Framework

Source: *https://www.coso.org*

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

Figure 22.2: COSO ERM framework

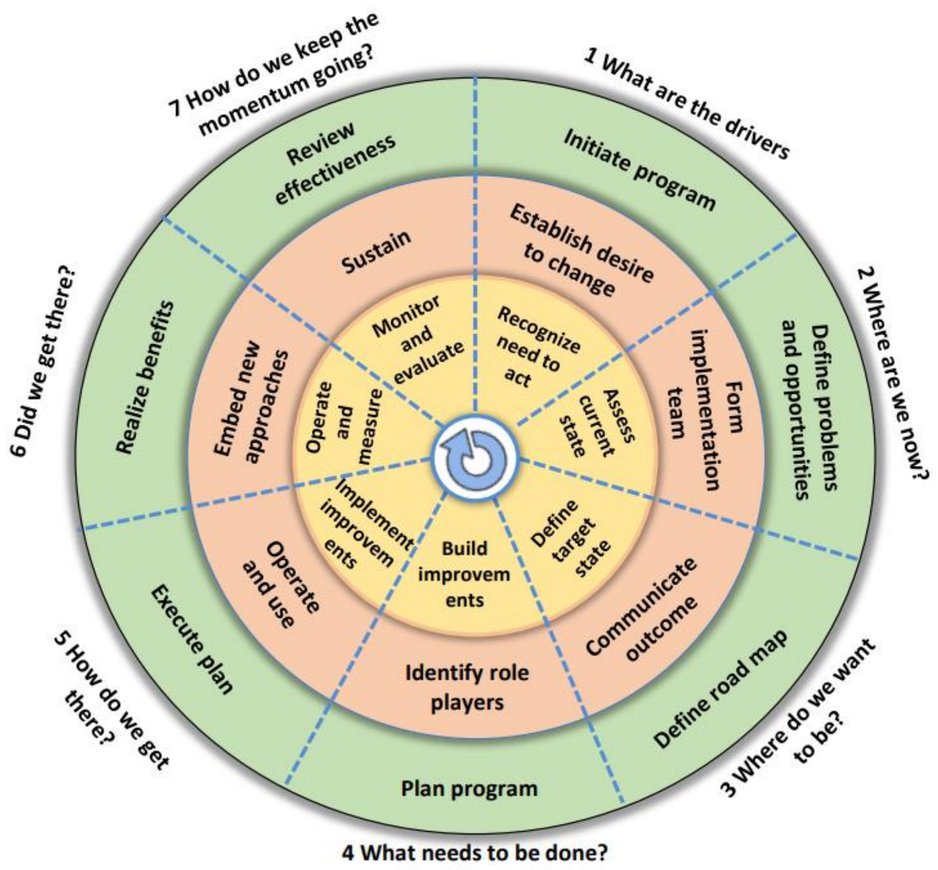
COSO ERM Components and Principles

- **Governance and Culture**: Governance sets an organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, ERM. Culture pertains to ethical values, desired behaviors, and an understanding of risk in the entity.

- **Strategy and Objective-Setting**: ERM, strategy and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
- **Performance:** Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. They are prioritized by severity in the context of risk appetite. An organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
- **Review and Revision:** By reviewing entity performance, an organization can consider how well the components of ERM function over time and in light of substantial changes, and, thereafter, what revisions are needed.
- **Information, Communication, and Reporting:** ERM requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across an organization.

COBIT Framework

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



https://www.isaca.org

COBIT Framework

Source: *https://www.isaca.org*

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

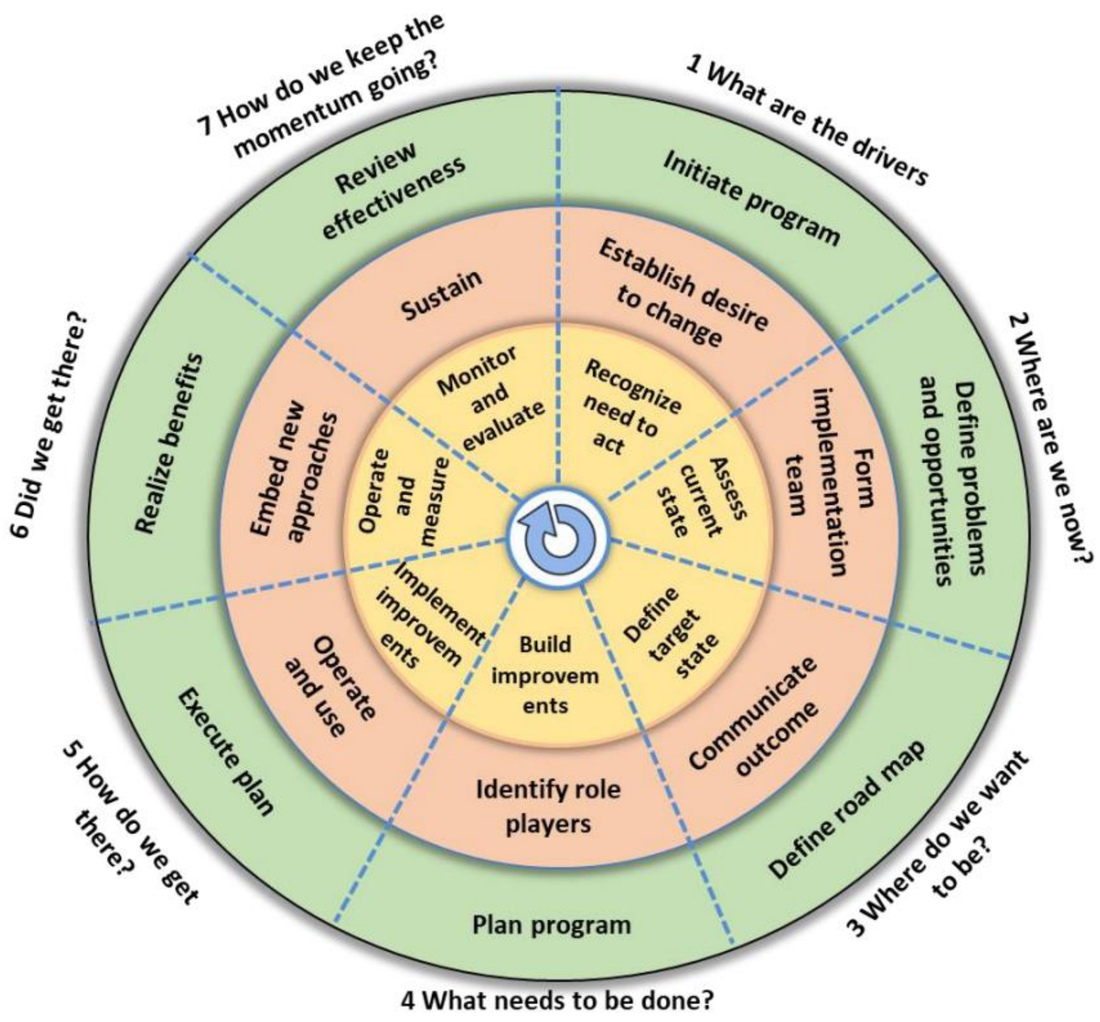


Figure 22.3: COBIT framework

COBIT helps enterprises of all sizes

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

COBIT Framework Internal Stakeholders

- **Risk Management:** Ensures the identification and management of all IT-related risk
- **Assurance Providers:** Manages dependencies on external service providers, provides IT assurance, and ensures an effective and efficient system of internal controls
- **IT Managers:** Provides guidance on how best to build and structure the IT department, manage performance of IT, run an efficient and effective IT operation, control IT costs, and align IT strategy to business priorities.
- **Business Managers:** Helps understand how to obtain the IT solutions that enterprises require and how best to exploit new technology for strategic opportunities
- **Executive Management:** Provides guidance on how to organize and monitor IT performance across the enterprise
- **Boards:** Provides insights on how to obtain value from the use of IT and explains relevant board responsibilities

COBIT Framework External Stakeholders

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

COBIT Framework Key Concept Principles

- **Governance System Principles:** The six principles are the core requirements for a governance system for enterprise information and technology.
- **Provide Stakeholders Value:** Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of IT.

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

Governance Framework Principles

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

Other Risk Management Frameworks

ISO 27005

- ISO 27005 provides information guidelines designed to provide broadly **acceptable guidance** for information security risk management
- The standard applies globally, supports wide adoption across industries, and maps directly to the strategy and recommendations outlined in ISO 27001

ISO 31000

- ISO 31000 is a framework that provides **generic guidelines** for enterprise risk management (ERM) with a universally recognized risk paradigm for practitioners and companies

Threat Agent Risk Assessment (TARA)

- TARA distills the immense number of possible information security attacks into a digest of only those exposures most likely to occur to support the development of optimal **security strategies**

Other Risk Management Frameworks (Cont'd)

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro	❑ OCTAVE Allegro is a lean **risk assessment method** and does not provide guidance in selecting security controls ❑ The framework supports a simple qualitative risk assessment and a **structured threat analysis**, primarily suitable for smaller organizations
FAIR representation of information Security Risk	❑ FAIR selects at least **one object** within an environment and quantifies the strength of its controls ❑ This is done by quantifying authentication controls, authorization controls, and then structural integrity
ITIL Risk Management	❑ ITIL is an acceptable solution to support information security risk management ❑ Formerly known as the Information Technology Infrastructure Library, ITIL is a set of practices for IT service management that focuses on **aligning IT services** with the needs of a business

Other Risk Management Frameworks

- **ISO 27005**

  Source: *https://www.iso.org*

  ISO 27005 provides information guidelines designed to provide broadly acceptable guidance for information security risk management. The standard applies globally, supports wide adoption across industries, and maps directly to the strategy and

recommendations outlined in ISO 27001. The ISO 27005 risk management workflow directs a structured sequence of steps to manage information security risks for a process, a system, or an enterprise.

ISO 27005 Risk Management Workflow

1. Design controls on the basis of risks clearly understood and measured (as much as possible) given existing threats that could potentially exploit vulnerabilities to organizational assets.
2. Systematic deployment of controls to reduce risks to an acceptable level of residual risk after approval by business leadership.
3. Manage controls to maintain an acceptable level of mitigation.
4. Provide ongoing analysis of controls to confirm continued effectiveness in light of changing operational conditions.

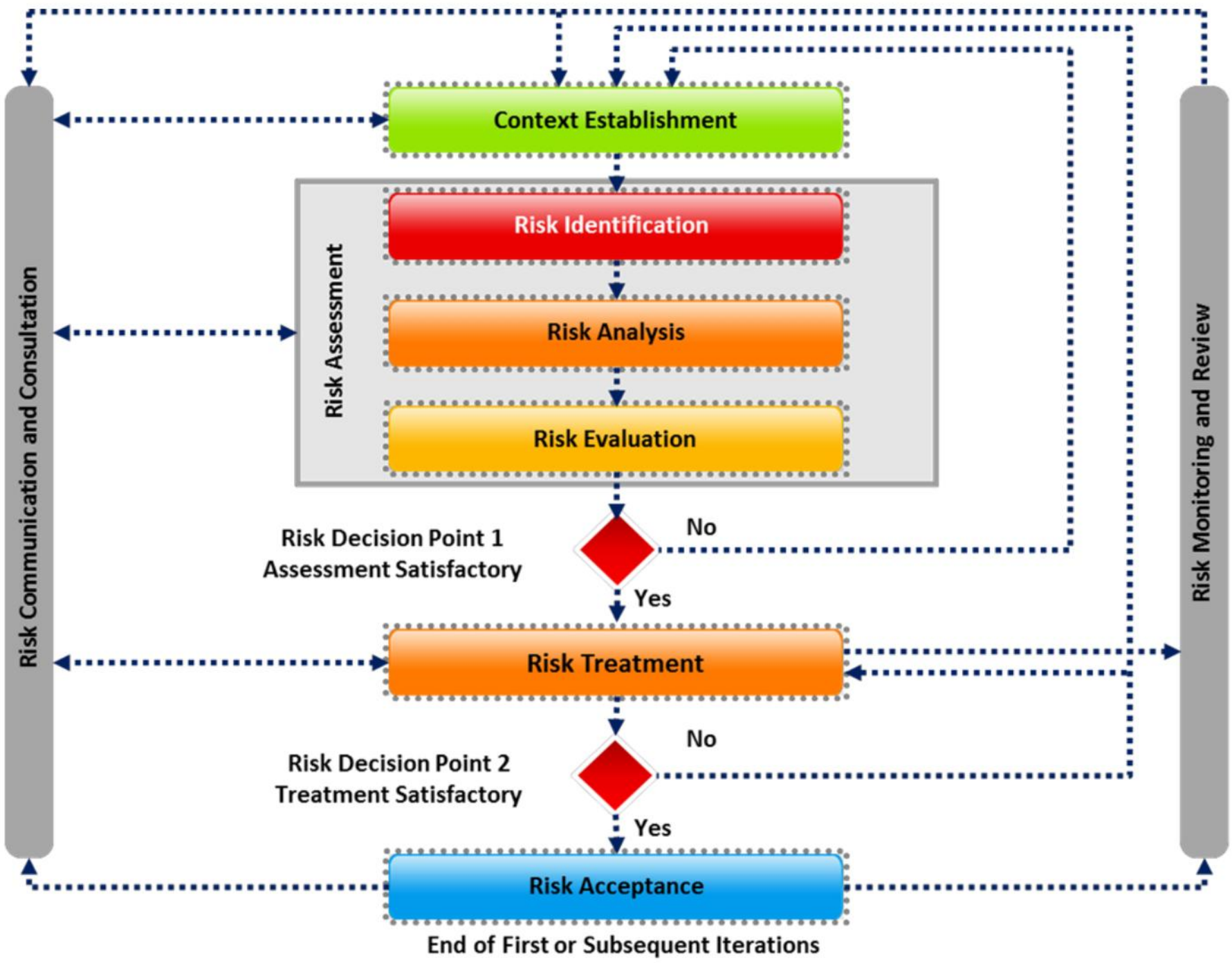


Figure 22.4: ISO 27005 Risk management workflow

- **ISO 31000**

  Source: *https://www.iso.org*

  ISO 31000 is a framework that provides generic guidelines for enterprise risk management (ERM) with a universally recognized risk paradigm for practitioners and

companies. The standard replaces a myriad of conflicting standards, methodologies, and paradigms that differ between industries, subject matters, and regions. A chief risk officer (CRO) is more likely to use ISO 31000 to manage enterprise risk; however, a security professional can use this framework as an alternative to ISO 27005 or another framework dedicated to information security risk management.

ISO 31000 is applicable and adaptable for any public, private, or community enterprise as well as any association, group, or individual. The scope of this standard is not limited to information security but extends to address all potential risks within an organization. It defines risk management practices using with an internationally recognized benchmark.

Three documents make up the ISO 31000 family:

- **ISO 31000:2009** Principles and Guidelines on Implementation
- **ISO/IEC 31010:2009** Risk Management–Risk Assessment Techniques
- **ISO Guide 73:2009** Risk Management–Vocabulary

- **Threat Agent Risk Assessment (TARA)**

  Source: *https://www.mitre.org*

  TARA distills the immense number of possible information security attacks into a digest of only those exposures most likely to occur to support the development of optimal security strategies. TARA identifies threat agents pursuing reasonably obtainable objectives that could cause unsatisfactory losses. The approach concentrates on threat agents and their motivations, methods of attack, attack objectives, and how they map to existing controls. It does not focus on weak points associated with specific vulnerabilities.

  Conducting TARA

  It would be prohibitively expensive and impractical to defend every possible vulnerability. By using a predictive methodology to prioritize specific areas of concern, we can both proactively target the most critical exposures and efficiently apply our resources for maximum results in information security risk management. Specifically, the TARA methodology identifies which threat agents pose the greatest risk, what they want to accomplish, and the likely methods they will employ. These methods are cross-referenced with existing vulnerabilities and controls to pinpoint the areas that are most exposed.

  The TARA methodology uses the following six steps to find the critical areas of exposure that an organization must address. By identifying the most important threat agents, objectives, and methods, the TARA methodology can help direct the information security strategy to the most critical exposures.

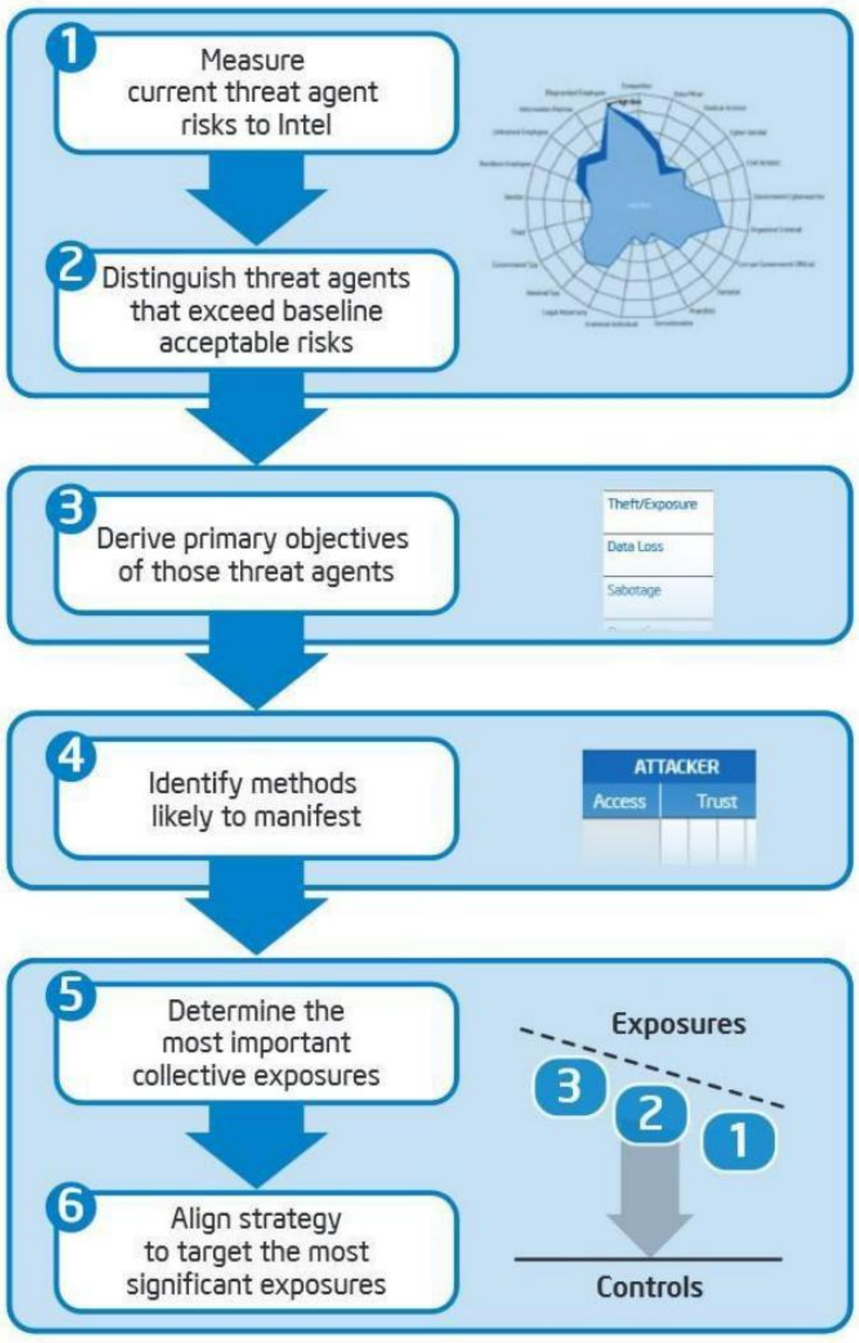


Figure 22.5: TARA methodology

- **Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro**

  Source: *https://ntrl.ntis.gov*

  OCTAVE Allegro is a lean risk assessment method and does not provide guidance in selecting security controls. The framework supports a simple qualitative risk assessment and a structured threat analysis, primarily suitable for smaller organizations.

  OCTAVE Allegro Roadmap

  OCTAVE Allegro consists of eight steps organized into four phases. The framework allows an organization to focus on the most important assets by ensuring they are selected for review through a systematic and consistent process. By focusing on information assets exclusively and other assets (such as people, technology, and facilities) through association with information assets, the organization has a better opportunity to define a manageable scope. This potentially reduces the effort required for threat identification, risk analysis, and mitigation planning.

  1. Develop risk measurement criteria consistent with the organization's mission, goal objectives, and critical success factors.
  2. Create a profile of each critical information asset that establishes clear boundaries for the asset, identifies its security requirements, and identifies its containers.

3. Identify threats to each information asset in the context of its containers.
4. Identify and analyze risks to information assets and begin to develop mitigation approaches

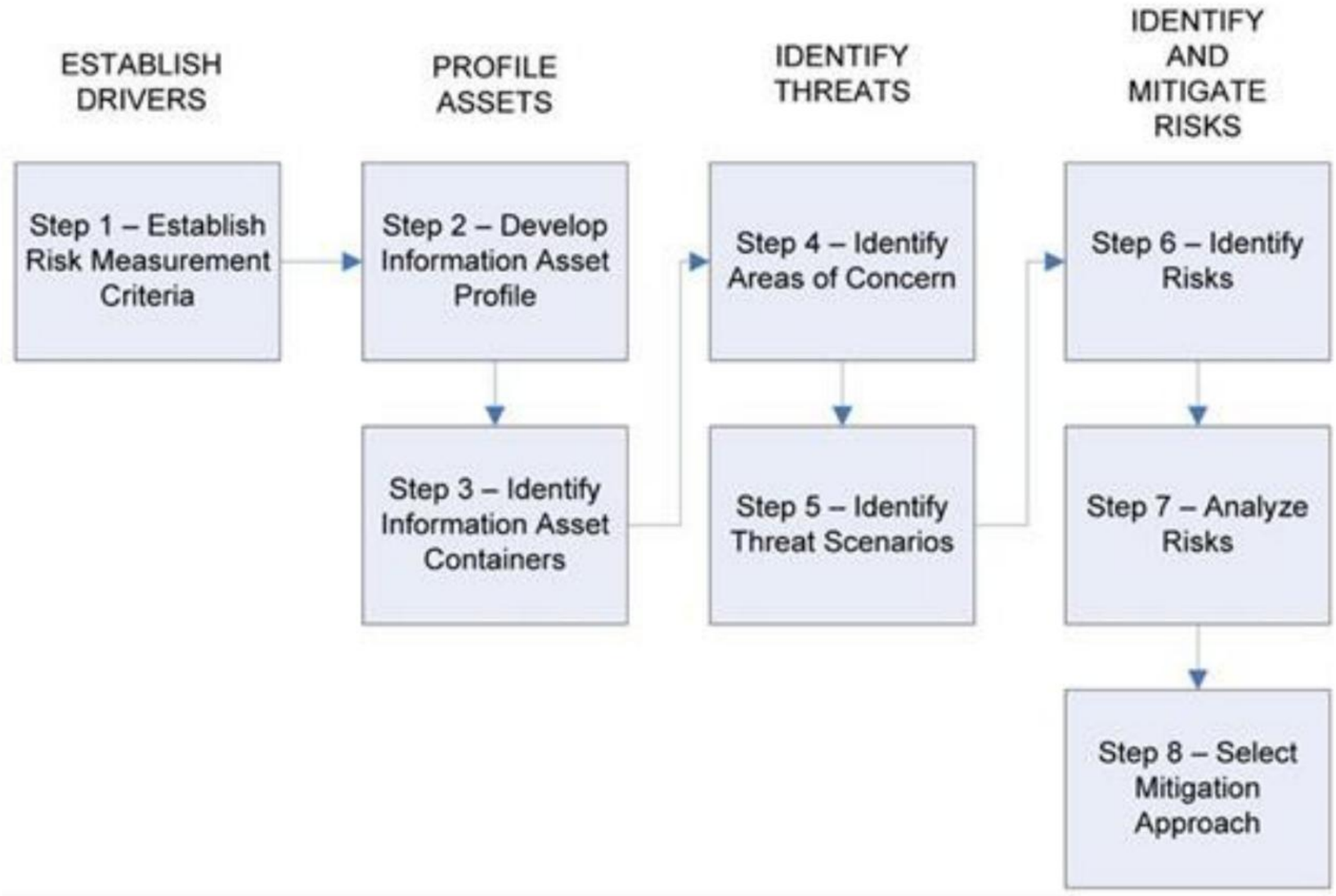


Figure 22.6: OCTAVE Allegro workflow

- **FAIR representation of information Security Risk**

  Source: *https://www.fairinstitute.org*

  FAIR is a tool that complements existing risk management frameworks by providing a model to understand, analyze, and quantify information risk in financial terms. FAIR's risk model components are specifically designed to support quantitative risk management.

  FAIR representation of information Security Risk

  FAIR selects at least one object within an environment and quantifies the strength of its controls. This is done by quantifying authentication controls, authorization controls, and then structural integrity. Next, global variables are set up for the environment. For example, determination is made as to whether the environment is subject to regulatory laws. Then, selecting at least one threat community, information risk is calculated.

  This calculation is accomplished by performing a statistical analysis using the strengths of controls on at least one object, the characteristics of at least one threat community, and the global variables of the environment. This is used to compute a value representing information risk.

  The method identifies the salient objects within a risk environment. It defines their characteristics, considering how they interact with each other. Using a statistically

sound mathematical calculation to emulate these interactions, FAIR derives probabilities. The method then represents the security risk as an integer, distribution, or some other variable.

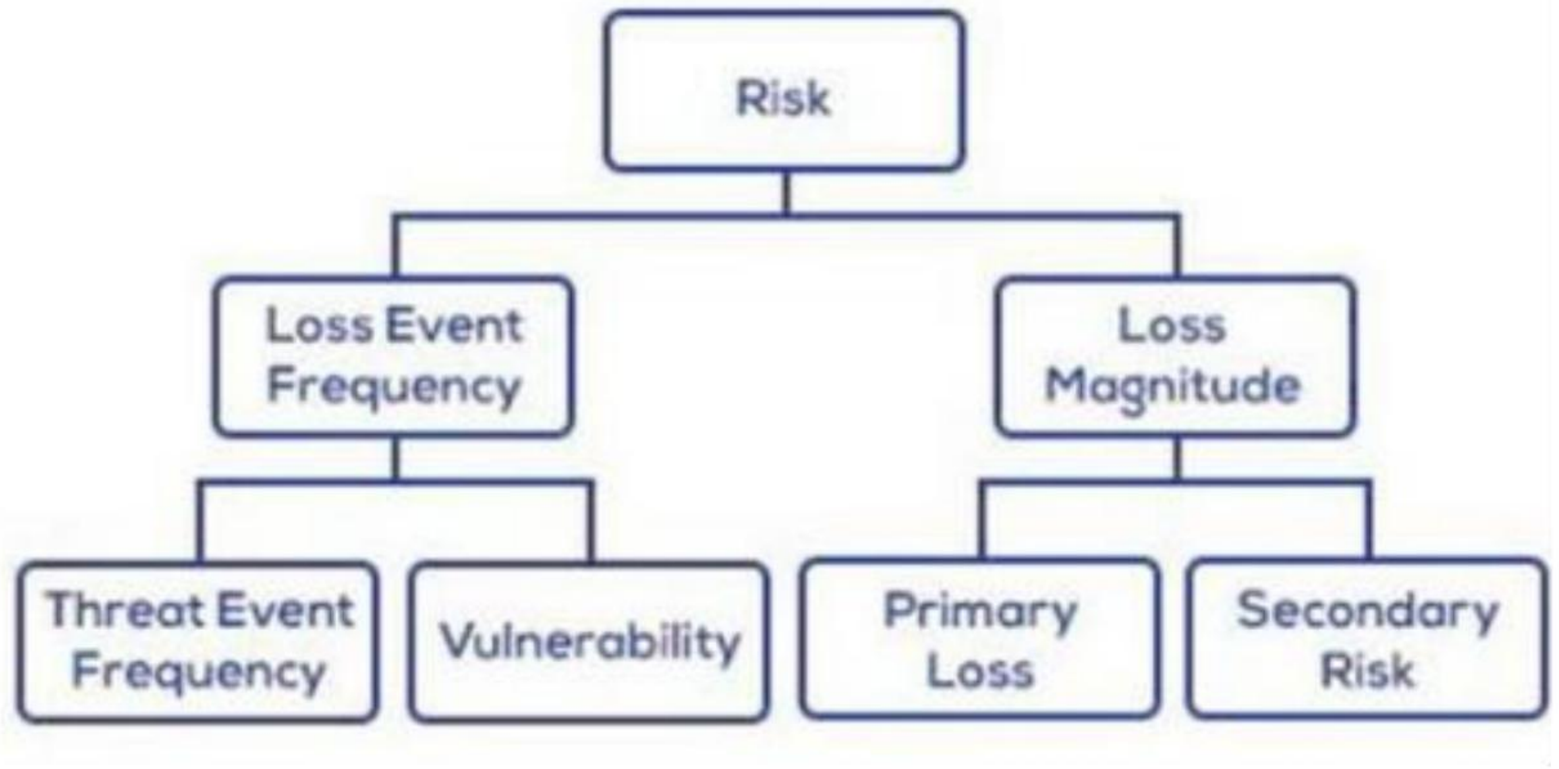
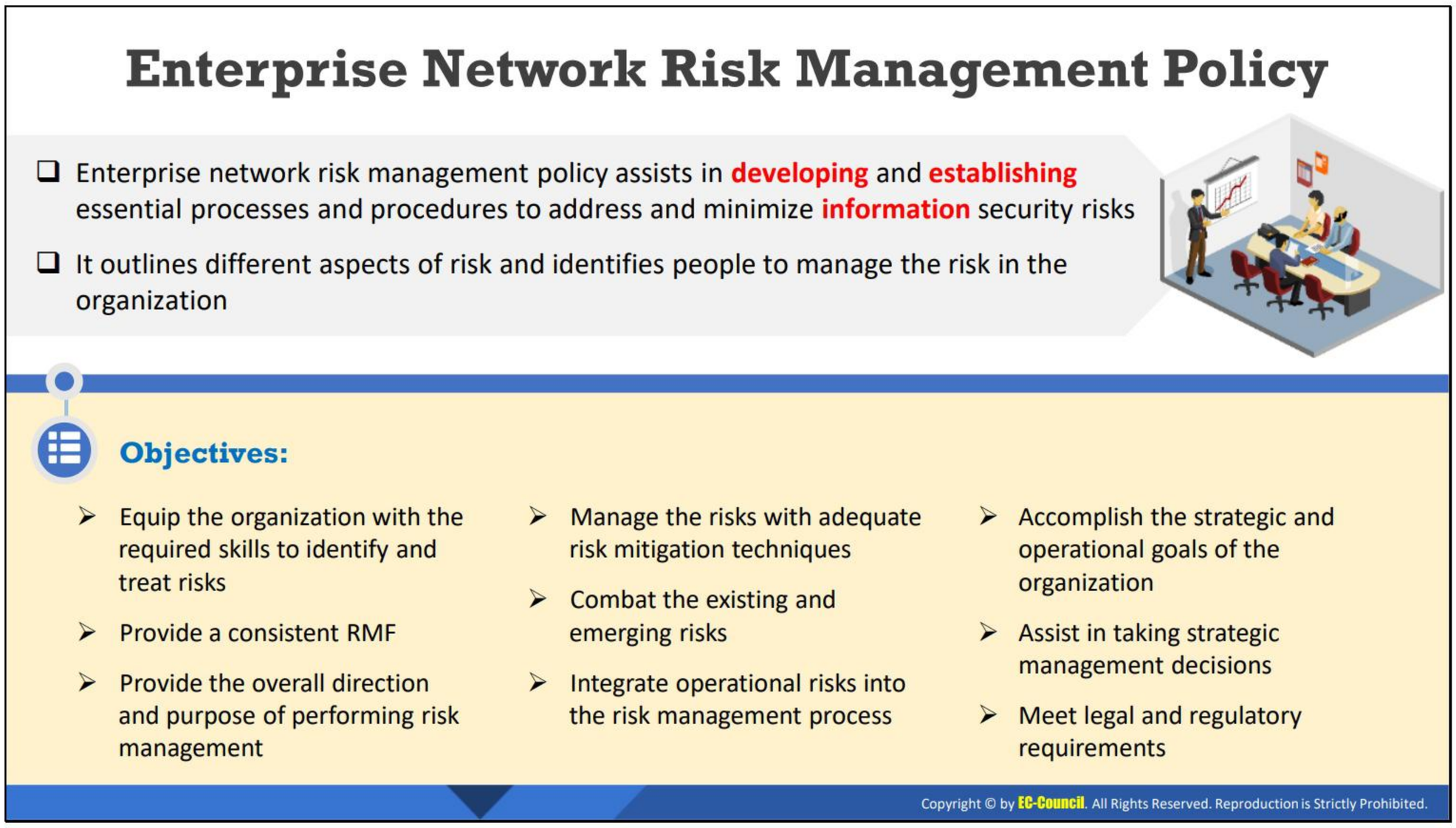


Figure 22.7: FAIR Risk Model

- **ITIL Risk Management**

  Source: *https://www.axelos.com*

  ITIL is an acceptable solution to support information security risk management. Formerly known as the Information Technology Infrastructure Library, ITIL is a set of practices for IT service management that focuses on aligning IT services with the needs of a business. Because business alignment is a security goal, a security professional can leverage mature IT service delivery practices to provide information security services to the organization. ITIL's Service Operation (SO) processes are particularly helpful to support security objectives by outlining best practices for delivering value in regard to event management, identity management, problem management, and incident management processes.



Enterprise Network Risk Management Policy

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

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

Objectives of Enterprise Network Risk Management Policy

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

Best Practices for Effective Implementation of Risk Management

Implementing ERM involves establishing a proper ERM system.

Best Practices for Effective Risk Management

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

Module Summary

This module discussed the concepts of risk management. It discussed various types of risks. It also discussed various risk management phases. Finally, this module provided an overview of various risk management frameworks.