EC-Council

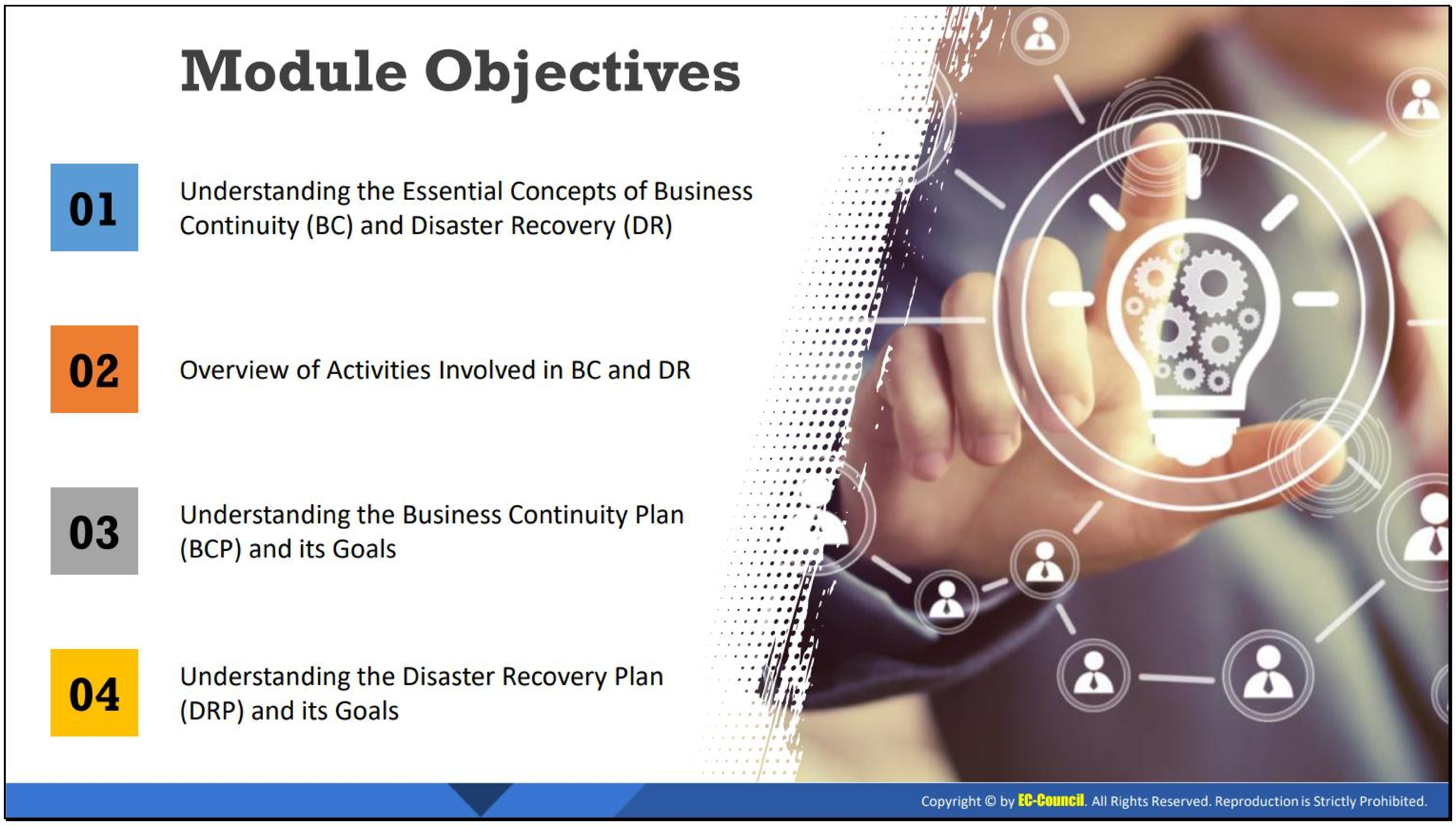
C|CT

Certified Cybersecurity Technician

Module - 21

Business Continuity and Disaster Recovery

This page is intentionally left blank.



Module Objectives

01 Understanding the Essential Concepts of Business Continuity (BC) and Disaster Recovery (DR)

02 Overview of Activities Involved in BC and DR

03 Understanding the Business Continuity Plan (BCP) and its Goals

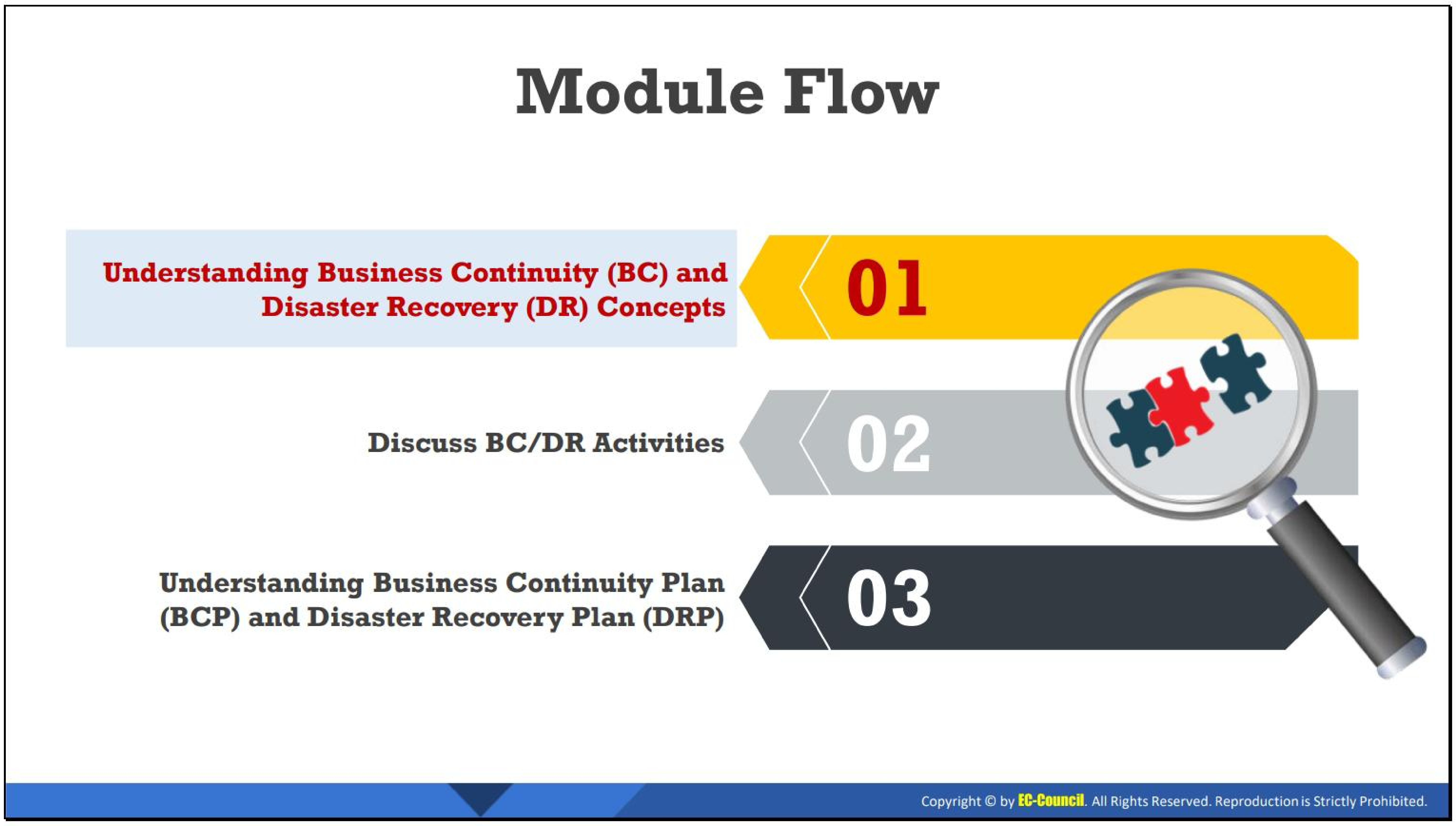
04 Understanding the Disaster Recovery Plan (DRP) and its Goals

Module Objectives

When threatened by a disruptive event, organizations should be capable of minimizing its impact, ensuring business continuity, and accelerating the disaster recovery process. As key personnel of an organization, security professionals should be well-acquainted with their organization's business continuity and disaster recovery plans so that they can restore business functions following a disaster.

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

- Understand the essential concepts of business continuity (BC) and disaster recovery (DR)
- Understand the activities involved in BC and DR
- Understand the BC plan (BCP) and its goals
- Understand the DR plan (DRP) and its goals



Module Flow

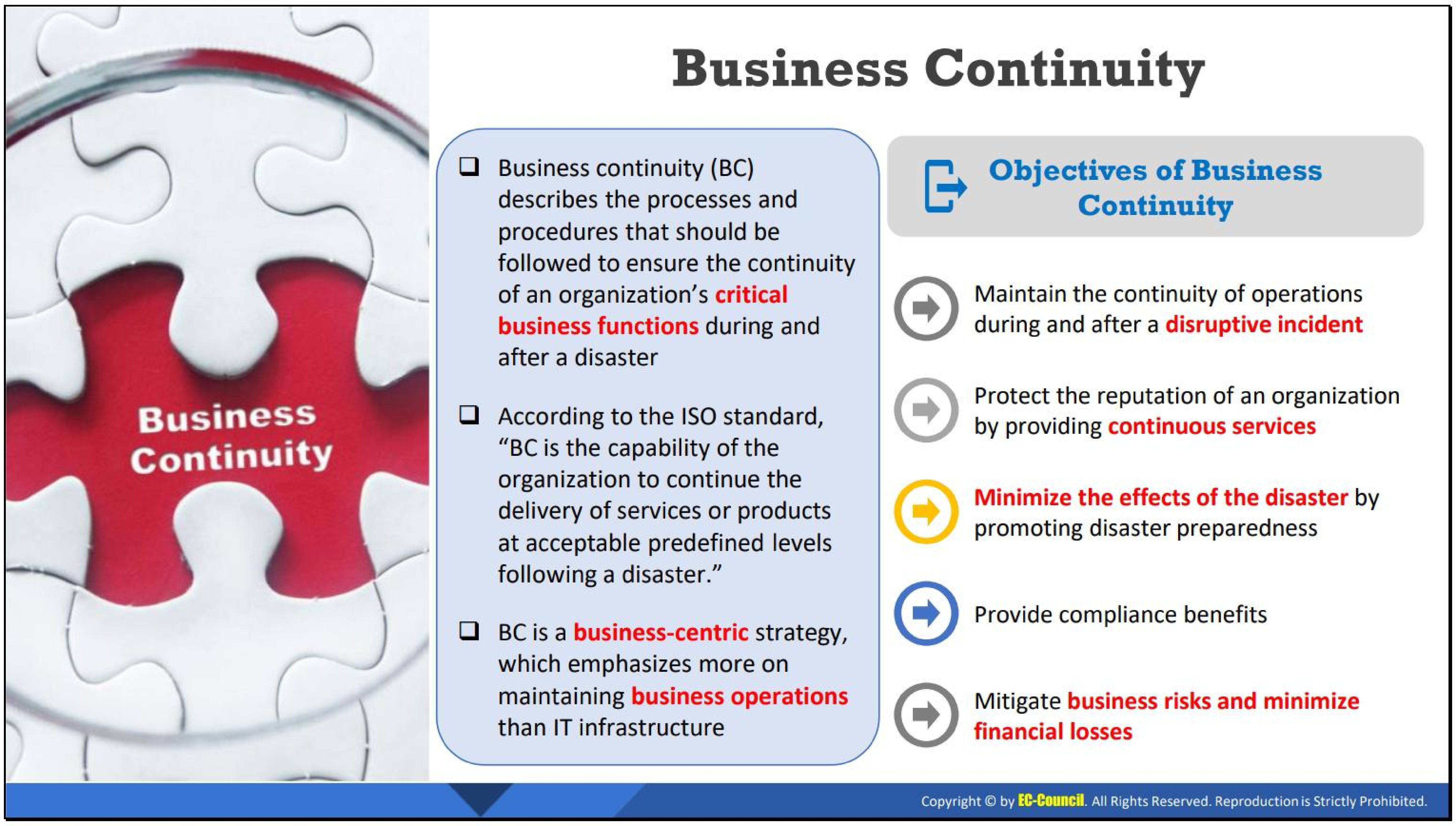
01 Understanding Business Continuity (BC) and Disaster Recovery (DR) Concepts

02 Discuss BC/DR Activities

03 Understanding Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

Understanding Business Continuity (BC) and Disaster Recovery (DR) Concepts

The objective of this section is to introduce terminologies associated with BC/DR such as business continuity, disaster recovery, business continuity management (BCM), business impact analysis (BIA), recovery time objective (RTO), and recovery point objective (RPO).


Business Continuity

Business Continuity

- ❑ Business continuity (BC) describes the processes and procedures that should be followed to ensure the continuity of an organization's **critical business functions** during and after a disaster
- ❑ According to the ISO standard, "BC is the capability of the organization to continue the delivery of services or products at acceptable predefined levels following a disaster."
- ❑ BC is a **business-centric** strategy, which emphasizes more on maintaining **business operations** than IT infrastructure

Objectives of Business Continuity

- Maintain the continuity of operations during and after a **disruptive incident**
- Protect the reputation of an organization by providing **continuous services**
- **Minimize the effects of the disaster** by promoting disaster preparedness
- Provide compliance benefits
- Mitigate **business risks and minimize financial losses**

Business Continuity

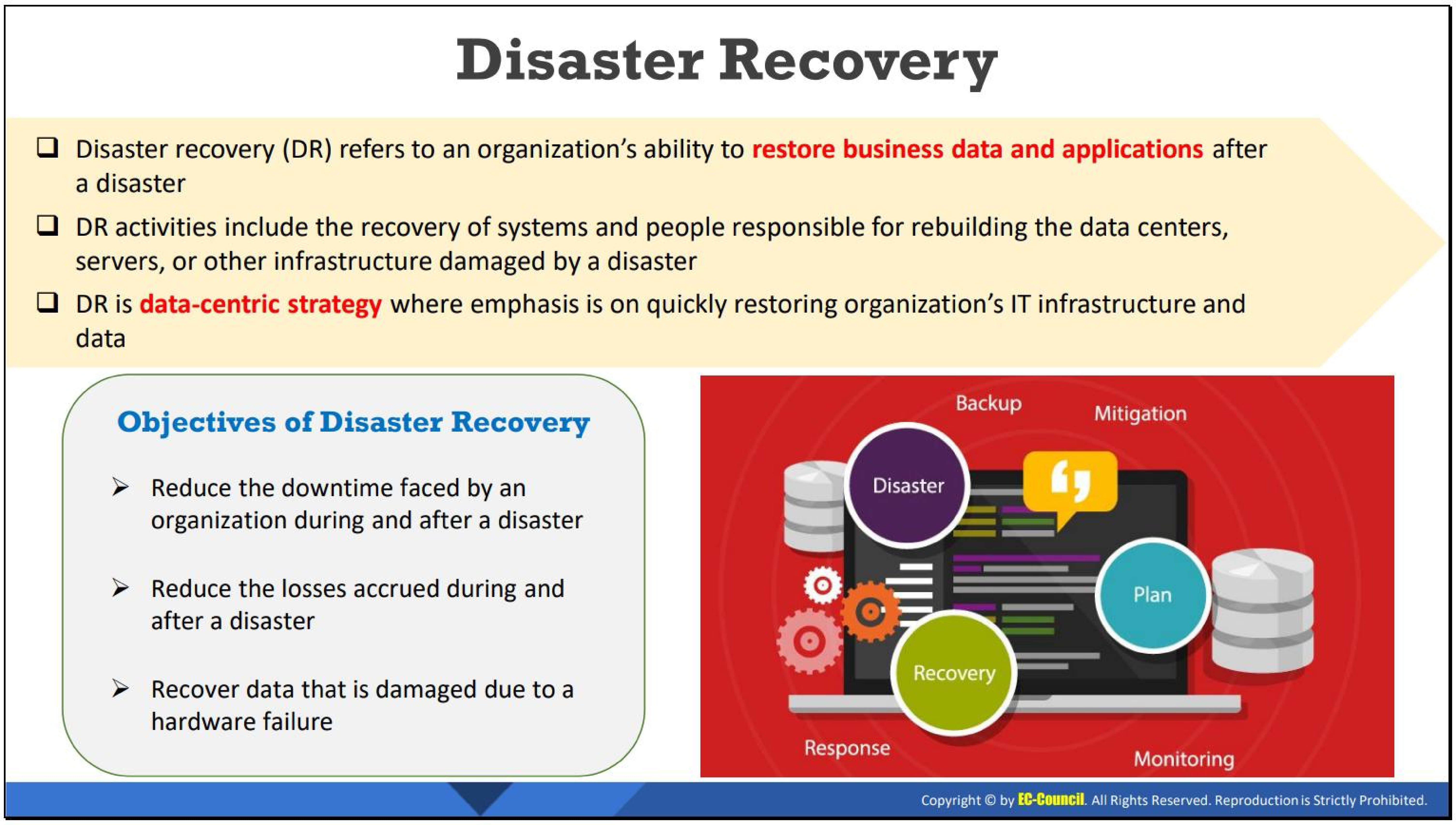
Business continuity is described as the processes, procedures, decisions, and activities that ensure continuity of organization's business function irrespective of the potential risk, threat, or cause of an outage. As per the standard set by the International Organization of Standardization (ISO), "BC is the capability of the organization to continue the delivery of services or products at acceptable predefined levels following a disaster." Hence, BC strategies aim at reducing the downtime following a disruption event. Business continuity is a business-centric strategy that emphasizes more on maintaining business operations. Business continuity strategies aim to reduce the downtime following a disruption event. In some organizations, downtime costs significantly exceed the cost of continuous availability; since these organizations are more exposed to losses, they have a higher motivation to spend on BC. In this context, it must be noted that fully redundant systems comprise a significant part of the BC spending. However, small-scale companies do not spend much on these systems owing to their low revenue generation. Regardless of the allocation, BC plays a significant role in organizations. Some of the objectives of BC are as follows:

Objectives of Business Continuity

- **Maintain the continuity of operations during and after a disruptive incident**: BC helps a company to continue its operations following a disaster, from a minor event to a major catastrophe such as hardware failure, virus and malware attacks, accidental damage, and natural disaster.
- **Protect organizational reputation by ensuring continuous service delivery**: Companies that fail to manage disasters appear incompetent to the public. A good BCP helps companies to manage disasters and ensures a smooth disaster recovery. It facilitates the

continuous delivery of a company's critical products and services while preserving its brand value and reputation.

- **Prepare organizations for disruptive events**: An organization must design an optimal plan to mitigate the effect of a disaster and continue its critical business functions, and BC helps organizations to prepare for such disruptive events.
- **Provide compliance benefits**: Organizations that are compliant with BC standards are perceived as reliable by the stakeholders.
- **Reduce business risks and financial losses**: BC reduces both business and financial risks. The risk of a data breach can be avoided by setting up a resilient network and robust backup capabilities, and a good BCP can mitigate the financial losses associated with a disaster.



Disaster Recovery

- ❑ Disaster recovery (DR) refers to an organization’s ability to **restore business data and applications** after a disaster
- ❑ DR activities include the recovery of systems and people responsible for rebuilding the data centers, servers, or other infrastructure damaged by a disaster
- ❑ DR is **data-centric strategy** where emphasis is on quickly restoring organization’s IT infrastructure and data

Objectives of Disaster Recovery

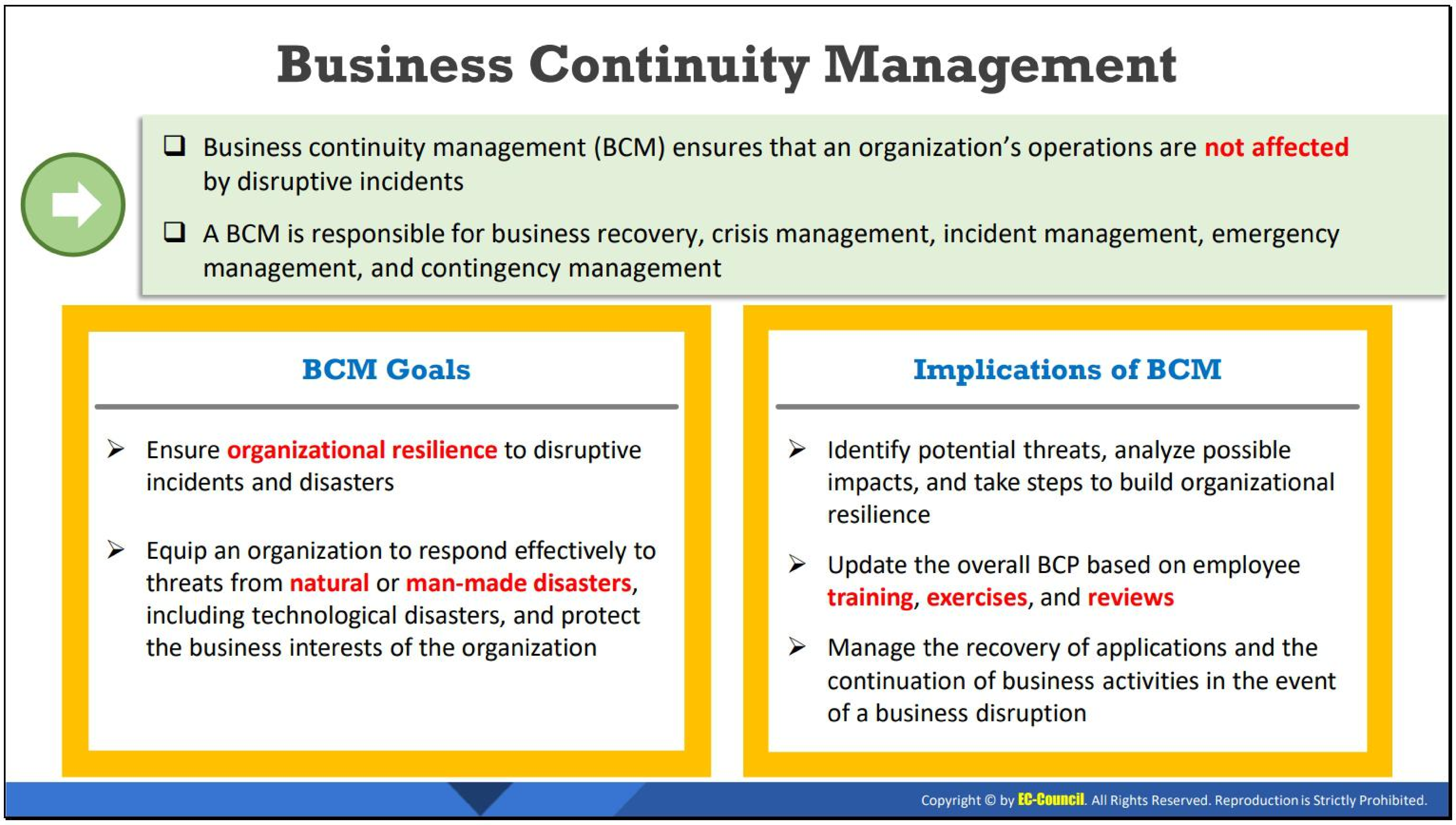
- ➢ Reduce the downtime faced by an organization during and after a disaster
- ➢ Reduce the losses accrued during and after a disaster
- ➢ Recover data that is damaged due to a hardware failure

Disaster Recovery

Careful security planning contributes toward mitigating the impact of disasters on organizations. Disaster recovery (DR) is an area of security planning that reflects an organization’s ability to restore business data and applications after a disaster. It involves a set of procedures and policies aimed at recovering or restoring the critical technology infrastructure following a disaster. Specifically, in the context of disaster management, it is a data-centric strategy focusing on the recovery and restoration of lost data, systems, IT, or people responsible for rebuilding the data centers, servers, or other critical components of the IT infrastructure. The objectives of DR are as follows:

Objectives of Disaster Recovery

- **Reduce the downtime faced by an organization during and after a disruptive event:** A longer recovery time worsens the effect of a disaster, which includes brand damage, customer dissatisfaction, and revenue loss. Therefore, an effective DRP should minimize the downtime and enable quick recovery from disruptions.
- **Reduce losses accrued during and after a disaster**: A good DR should mitigate disruptions in business operations and minimize the losses associated with a disaster.
- **Recover the lost data**: Data are lost due to a hardware failure, virus and malware attacks, accidental damage, and natural disaster. DR aims to restore the business data following a disaster.



Business Continuity Management

❑ Business continuity management (BCM) ensures that an organization's operations are **not affected** by disruptive incidents

❑ A BCM is responsible for business recovery, crisis management, incident management, emergency management, and contingency management

BCM Goals

- Ensure **organizational resilience** to disruptive incidents and disasters
- Equip an organization to respond effectively to threats from **natural** or **man-made disasters**, including technological disasters, and protect the business interests of the organization

Implications of BCM

- Identify potential threats, analyze possible impacts, and take steps to build organizational resilience
- Update the overall BCP based on employee **training**, **exercises**, and **reviews**
- Manage the recovery of applications and the continuation of business activities in the event of a business disruption

Business Continuity Management

Business continuity management (BCM) is a process that ensures the continuity of business operations after disruptive incidents. A BCM is responsible for business recovery, crisis management, incident management, emergency management, and contingency management. The framework of BCM enables organizations to anticipate risks and internal and external threats. Organizations that implement a BCM program respond in a timely and effective manner to security incidents or natural disasters.

BCM includes the following:

- **Crisis management**: Crisis Management (CM) is the ability of an organization to respond under crisis, and thereby minimize the damage to its brand name, business operation, and revenue. A delay in the expedition of the CM plan by the senior management causes an overlap between the plans and responsibilities of the CM and BC processes.

- **Incident management**: Incident Management (IM) enables an organization to analyze, identify, and respond to and prevent such incidents. In a structured organization, these incidents fall under the purview of the Incident Management Team (IMT), the Incident Command System (ICS), or the Incident Response Team (IRT). The lack of effective incident management may disrupt business operations as well as stakeholders.

- **Contingency planning**: Organizations execute a contingency plan when their regular business operations are interrupted by a disruptive event. Contingency plans ensure continuous and prompt product and service delivery, on-site and off-site business operations, and customer satisfaction.

- **Business recovery**: Business recovery refers to an advance plan, arrangement, and procedure implemented by the bronze or operational teams of an organization after a disaster. It aims to recover the organization’s business processes around workspaces, personnel, equipment, and facilities, among others.

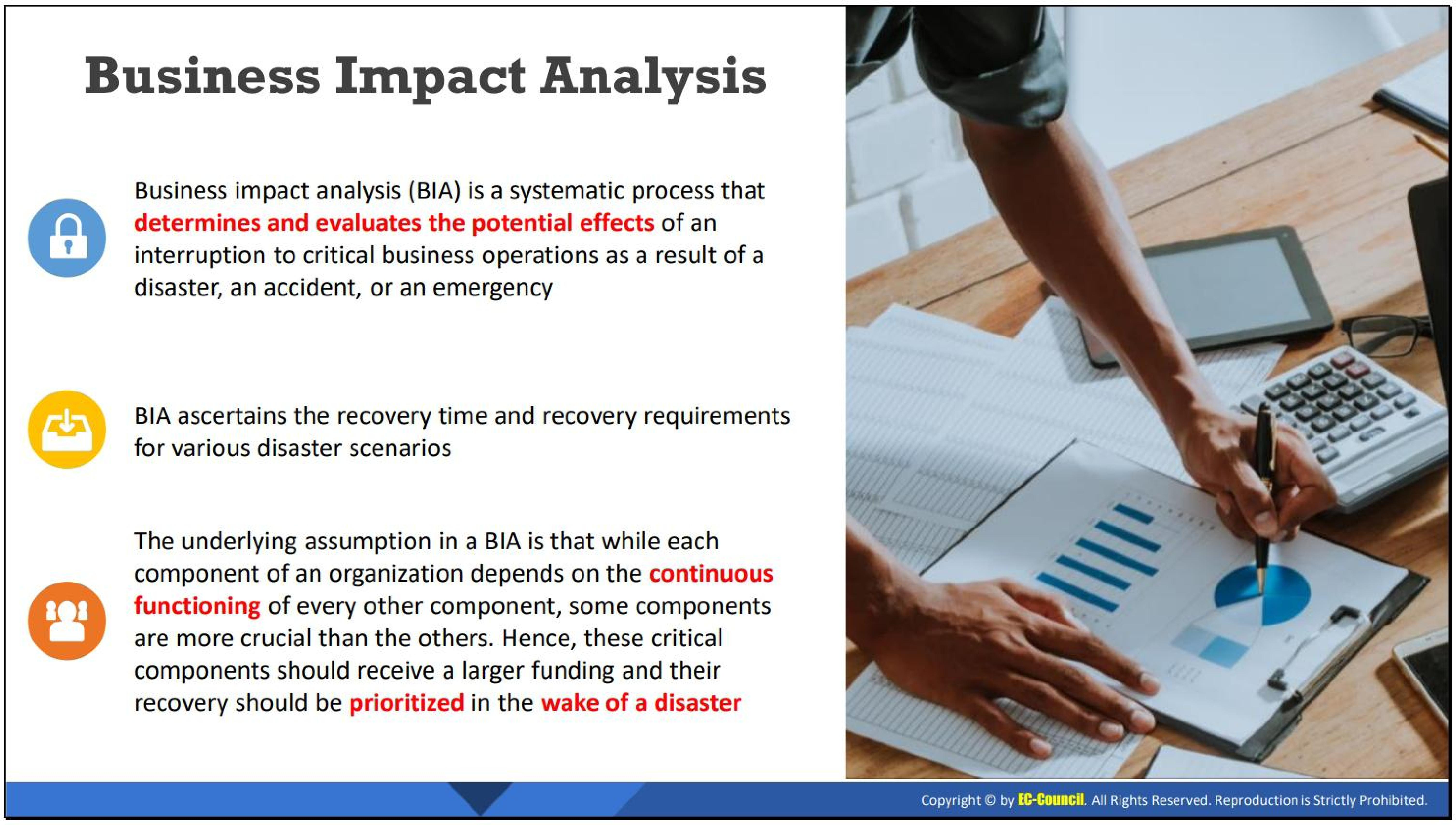
- **Emergency management**: It refers to the procedures and actions implemented after a crisis in order to safeguard people from harm.
- **DR**: It is a plan to restore important support systems such as hardware, IT assets, and communications, in order to reduce business downtime and accelerate the restoration of business operations.

Goals of Business Continuity Management

- **Ensure organizational resilience to disruptive incidents and disasters:** The security requirements of an organization can be ascertained through a business impact analysis and CM, DRP, and BCP. These plans should motivate employees to contribute collectively toward improving their organization’s resilience posture. It must be noted that employees play a significant role in helping organizations develop resilience.
- **Equip organizations to develop an effective response to threats:** Organizations face threats from natural or man-made disasters such as technological disaster. An effective BCM program can protect the business interests of an organization. It can introduce appropriate resilience strategies to reduce the impact of threats and contribute toward the formulation of plans to respond to and recover from threats that cannot be mitigated or controlled.

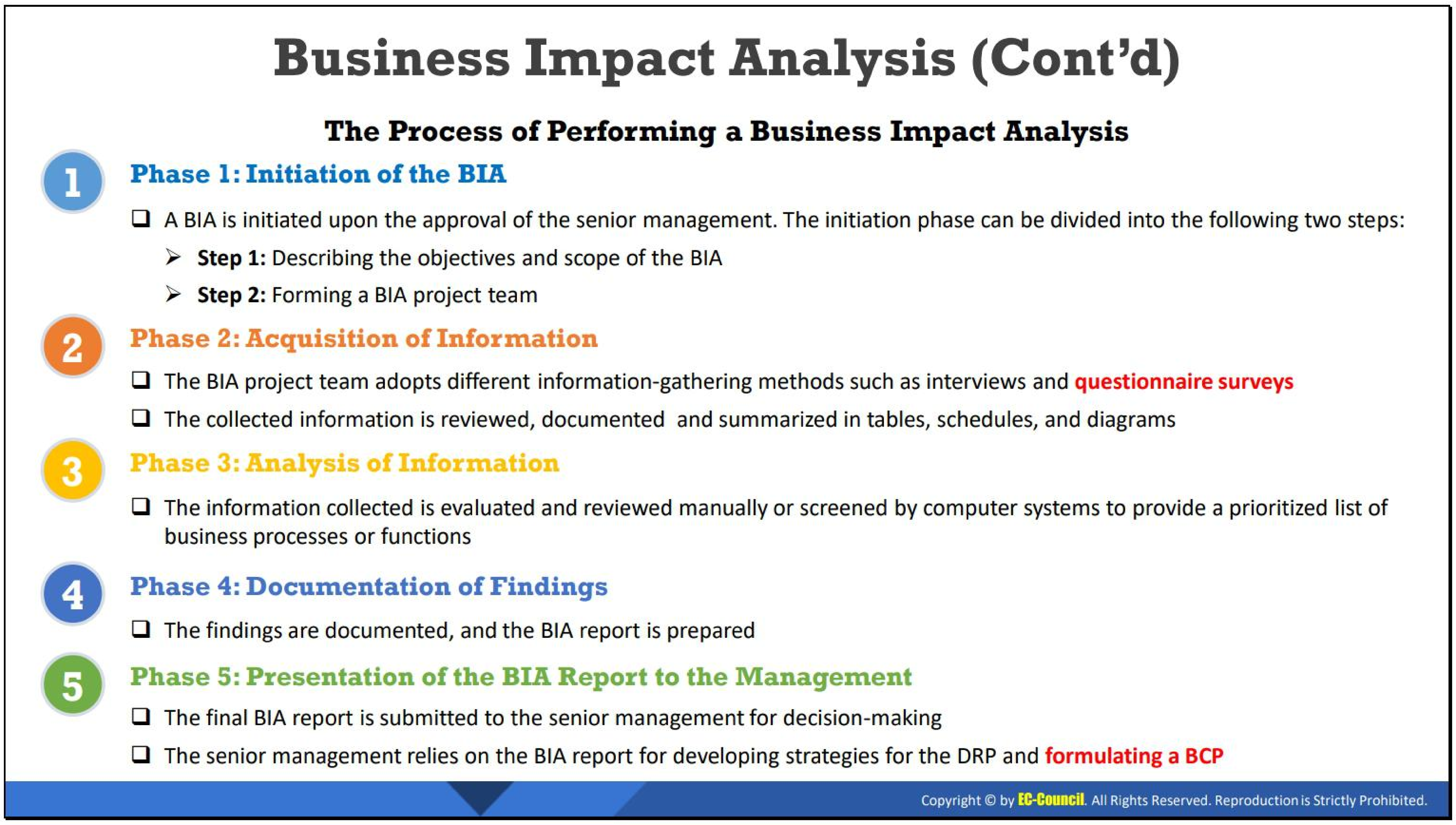
Implications of Business Continuity Management

- BCM ensures continuous operations and delivery of products and services at predefined levels during any disaster This is achieved by identifying potential threats, analyzing possible impacts, and taking steps to build organizational resilience.
- BCM safeguards the interest of an organization’s stakeholders, personnel, brand equity, and reputation. During a disaster, BCM ensures the effective execution of the DR and BC processes; the implementation of training programs, exercises, and reviews; and the upgradation of the BCP.
- BCM ensures that business applications are accessible to an organization’s customers even during disasters.



Business Impact Analysis

- Business impact analysis (BIA) is a systematic process that **determines and evaluates the potential effects** of an interruption to critical business operations as a result of a disaster, an accident, or an emergency
- BIA ascertains the recovery time and recovery requirements for various disaster scenarios
- The underlying assumption in a BIA is that while each component of an organization depends on the **continuous functioning** of every other component, some components are more crucial than the others. Hence, these critical components should receive a larger funding and their recovery should be **prioritized** in the **wake of a disaster**



Business Impact Analysis (Cont'd)

The Process of Performing a Business Impact Analysis

1 **Phase 1: Initiation of the BIA**

❑ A BIA is initiated upon the approval of the senior management. The initiation phase can be divided into the following two steps:

➢ **Step 1:** Describing the objectives and scope of the BIA

➢ **Step 2:** Forming a BIA project team

2 **Phase 2: Acquisition of Information**

❑ The BIA project team adopts different information-gathering methods such as interviews and **questionnaire surveys**

❑ The collected information is reviewed, documented and summarized in tables, schedules, and diagrams

3 **Phase 3: Analysis of Information**

❑ The information collected is evaluated and reviewed manually or screened by computer systems to provide a prioritized list of business processes or functions

4 **Phase 4: Documentation of Findings**

❑ The findings are documented, and the BIA report is prepared

5 **Phase 5: Presentation of the BIA Report to the Management**

❑ The final BIA report is submitted to the senior management for decision-making

❑ The senior management relies on the BIA report for developing strategies for the DRP and **formulating a BCP**

Business Impact Analysis

The business impact analysis (BIA) systematically evaluates and determines the potential effects of an interruption to critical business operations due to emergencies and accidents such as labor disputes, supplier failure, political turmoil, terrorist attacks, natural or man-made disasters, cyberattacks, and utility failures. Since the BIA focuses on minimizing the effects of the aforementioned risks, it should be included in the BCP. Specifically, the BIA has a planning and an exploratory component; the former focuses on risk-reduction strategies, and the latter identifies vulnerabilities. The BIA results in a report that helps an organization to determine potential risks and their impacts on its critical assets. In other words, the BIA report provides a comprehensive description of the risks and their impacts on business operations after a disruption. The basic assumption behind the BIA is that every component of an organization depends on the continuous functioning of all other components. However, certain components play a more important role, and hence need a larger allocation of funds following a disruption.

Overall, the due diligence assessment of the BIA helps an organization to develop a strategic plan of action for recovering from adverse events. Hence, businesses conduct a BIA to enhance the robustness of their DR program.

Reasons for Conducting Business Impact Analysis

- BIA assists in decision-making in the event of operational interruptions caused by disasters.
- BIA helps in the allocation of resources during the non-operational period.
- BIA provides the criteria for testing an organization's recovery plans.

The Process of Performing a Business Impact Analysis

There are no fixed guidelines for conducting a BIA. Based on the overall manner of execution in most companies, the multi-phase BIA process can be elaborated as follows:

- **Phase 1: Initiation of the BIA**

  A BIA is initiated upon the approval of the senior management. The initiation phase can be divided into the following two steps.

  - **Step 1: Describing the objectives and scope of the BIA**

    Organizations should clarify the objective for conducting a BIA.

  - **Step 2: Forming a BIA project team**

    The senior management should form a separate for conducting a BIA analysis. For this purpose, the management can either recruit skilled and knowledgeable personnel internally or outsource the BIA to third parties.

- **Phase 2: Acquisition of Information**

  The BIA project team can adopt different information-gathering methods such as interviews and questionnaire surveys. Questionnaires are extensively used as survey tools; in the given context, a questionnaire consists of a set of targeted questions that aim to assess the potential effects of interruption or disruption and determine assets that are critical to different business functions.

  The collected information is reviewed and documented in a clear and coherent manner, which is re-evaluated for accuracy. This information is summarized in tables, schedules, and diagrams.

- **Phase 3**: **Analysis of Information**

  The information collected is evaluated and reviewed manually or screened by computer systems.

  The objectives of reviewing the information are as follows:

  - To provide a prioritized list of business processes or functions, placing the most important ones on the top of the list.
  - To determine the technology and personnel required for maintaining the operations at an optimal level.
  - To establish the length of time or recovery time frame required to recover the function or process and restore organizational operations.

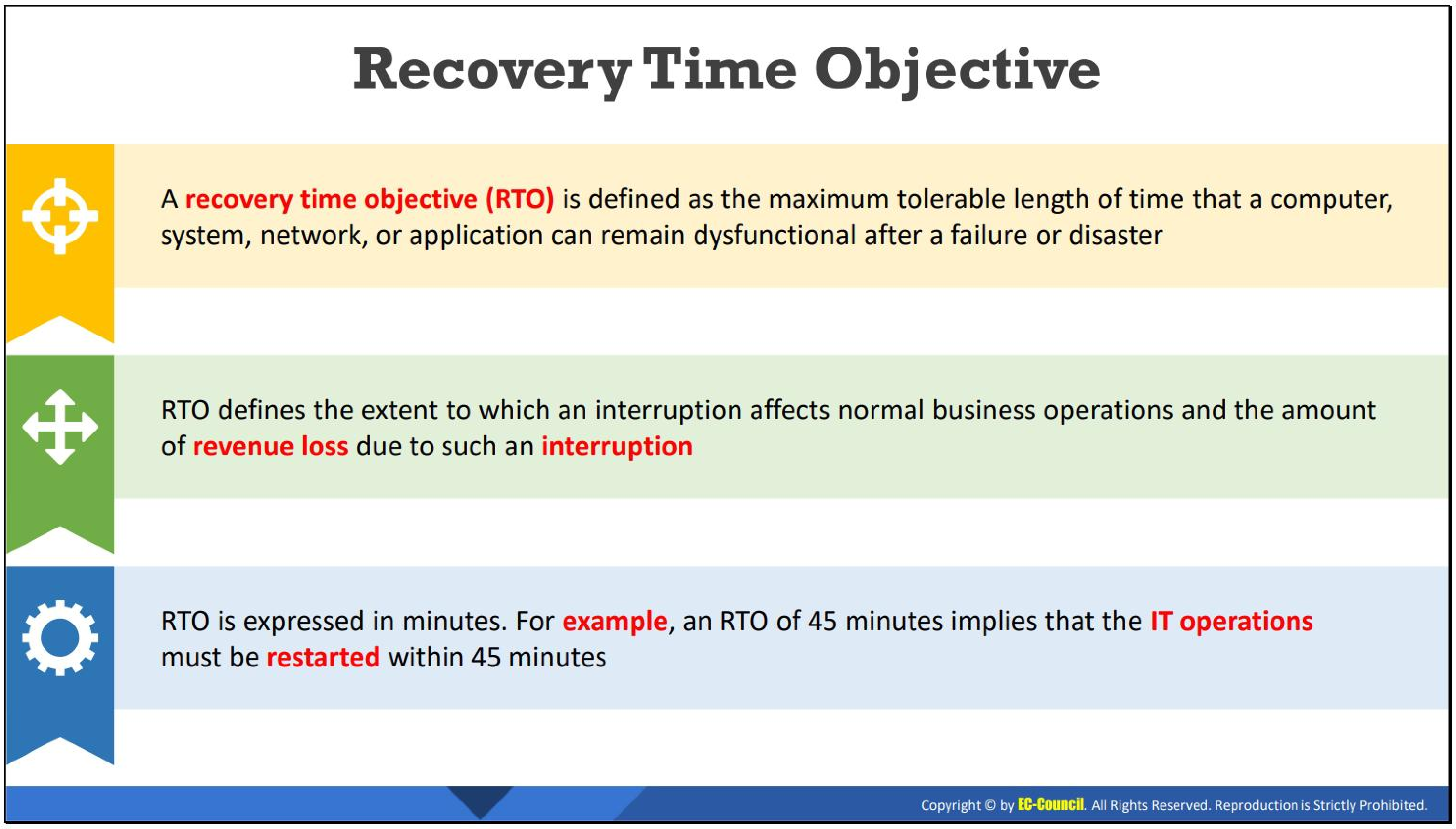
- **Phase 4: Documentation of Findings**

  In this phase, the findings are documented and the BIA report is prepared.

- **Phase 5: Presentation of the BIA Report to the Management**

  The final BIA report is submitted to the senior management for decision-making. The senior management relies on the BIA report for developing strategies for the DRP and formulating a BCP.

  Since a BIA examines the recovery point objectives (RPOs) and the recovery time objectives (RTOs), it serves as a starting point for developing a DR strategy.



Recovery Time Objective

A **recovery time objective (RTO)** is defined as the maximum tolerable length of time that a computer, system, network, or application can remain dysfunctional after a failure or disaster

RTO defines the extent to which an interruption affects normal business operations and the amount of **revenue loss** due to such an **interruption**

RTO is expressed in minutes. For **example**, an RTO of 45 minutes implies that the **IT operations** must be **restarted** within 45 minutes

Recovery Time Objective

A recovery time objective (RTO) is defined as the maximum tolerable length of time that a computer, system, network, or application can remain dysfunctional after a failure or disaster. These disruptions or outage can also be attributed to single points of failures that can be minimized by reducing the number of dependencies in a system or application design, implying that a weakness in one point cannot impact other points. Established by the process owner during the BIA, an RTO is a metric that calculates how fast an organization can recover its services and the IT infrastructure following a disaster event. It also calculates the mean time to repair the glitch for restoring business operations. It can be defined as the mean time for replacement or recovery. In other words, it measures the time taken by an organization to return to its pre-disaster operational levels. It is measured in seconds, minutes, hours, or days. An RTO of 45 min indicates that an organization can maintain its operations for that duration after the disruption of its infrastructure and the resulting data loss. If the organization fails to restore the infrastructure and data within 45 minutes, then the business may suffer an irreparable loss. Thus, RTO determines the extent to which a disaster interrupts normal operations and the resulting loss of revenue per unit time; hence, it is crucial to the DRP. These factors entirely depend on the affected application(s) and the equipment.

Several studies have been conducted to identify the cost of application downtime. The studies have indicated that the cost depends on the immediate, short-term, and tangible factors as well as on the long-term and intangible effects. In this context, it must be noted that the right DR technologies can minimize the downtime costs. Pre-defining the RTO for an application can help a security professional to determine the suitable DR technologies that can restore the application after a disruption. For example, redundant data backup on external hard drives may be the best DR solution for an application with an RTO of 60 minutes. Similarly, offsite storage on a remote web server or a recordable compact disk may be best suited for an application with an RTO of 4 days (96 hours).

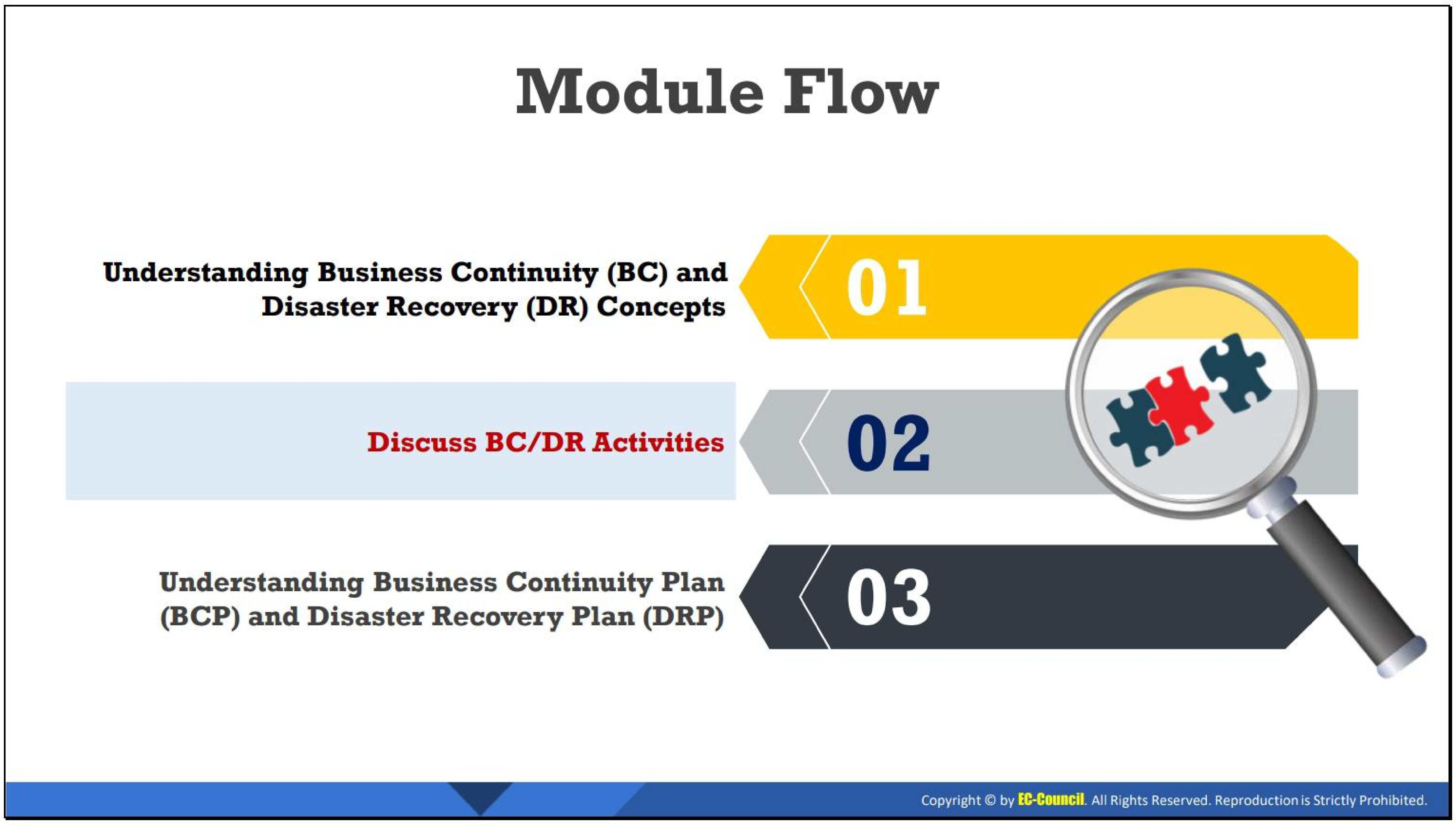
Recovery Point Objective

- **Recovery point objective (RPO)** is the maximum time frame for which an organization loses data after a major IT outage
- RPO provides a **foundation** for designing DR and BC solutions
- Every organization must calculate how long it can operate without the required data before suffering a failure

Recovery Point Objective

A recovery point objective (RPO) is the maximum time frame for which an organization loses data after a major IT outage. It determines the acceptable amount of data loss an enterprise can suffer in case of a disruption. An RPO sets goals for designing a BC, a DR, or high availability (HA), and hence it is crucial to DRP. Expressed in seconds, minutes, hours, or days, RPO can be measured from the time the hosting services become unavailable.

Pre-defining an RPO for a given system can help in determining the minimum frequency of backup. Like an RTO, an RPO allows the security professional to choose optimal procedures and DR technologies for a system. For example, 3-hourly-backups on external redundant hard drives are suitable for a system with an RPO of 3 hours. Similarly, backups at an interval of 96 hours on a recordable compact disk or tape are considered suitable for a system with an RPO of 4 days (96 hours).



Module Flow

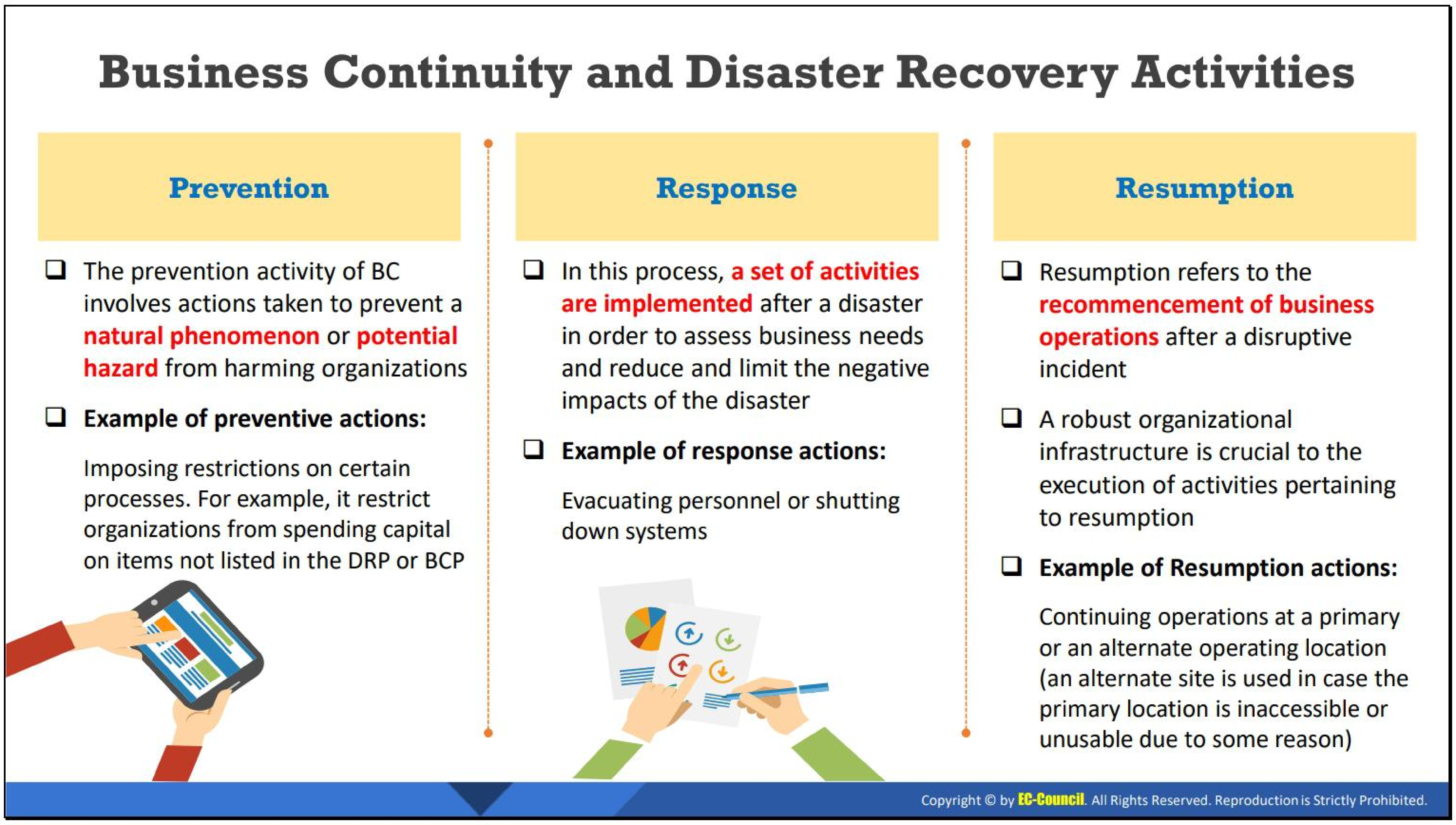
01 **Understanding Business Continuity (BC) and Disaster Recovery (DR) Concepts**

02 **Discuss BC/DR Activities**

03 **Understanding Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)**

Discuss BC/DR Activities

The objective of this section is to discuss the prevention, response, resumption, recovery, and restoration activities carried out as part of the BC and DR operations.



Business Continuity and Disaster Recovery Activities

Prevention

- ❑ The prevention activity of BC involves actions taken to prevent a **natural phenomenon** or **potential hazard** from harming organizations
- ❑ **Example of preventive actions:**

  Imposing restrictions on certain processes. For example, it restrict organizations from spending capital on items not listed in the DRP or BCP

Response

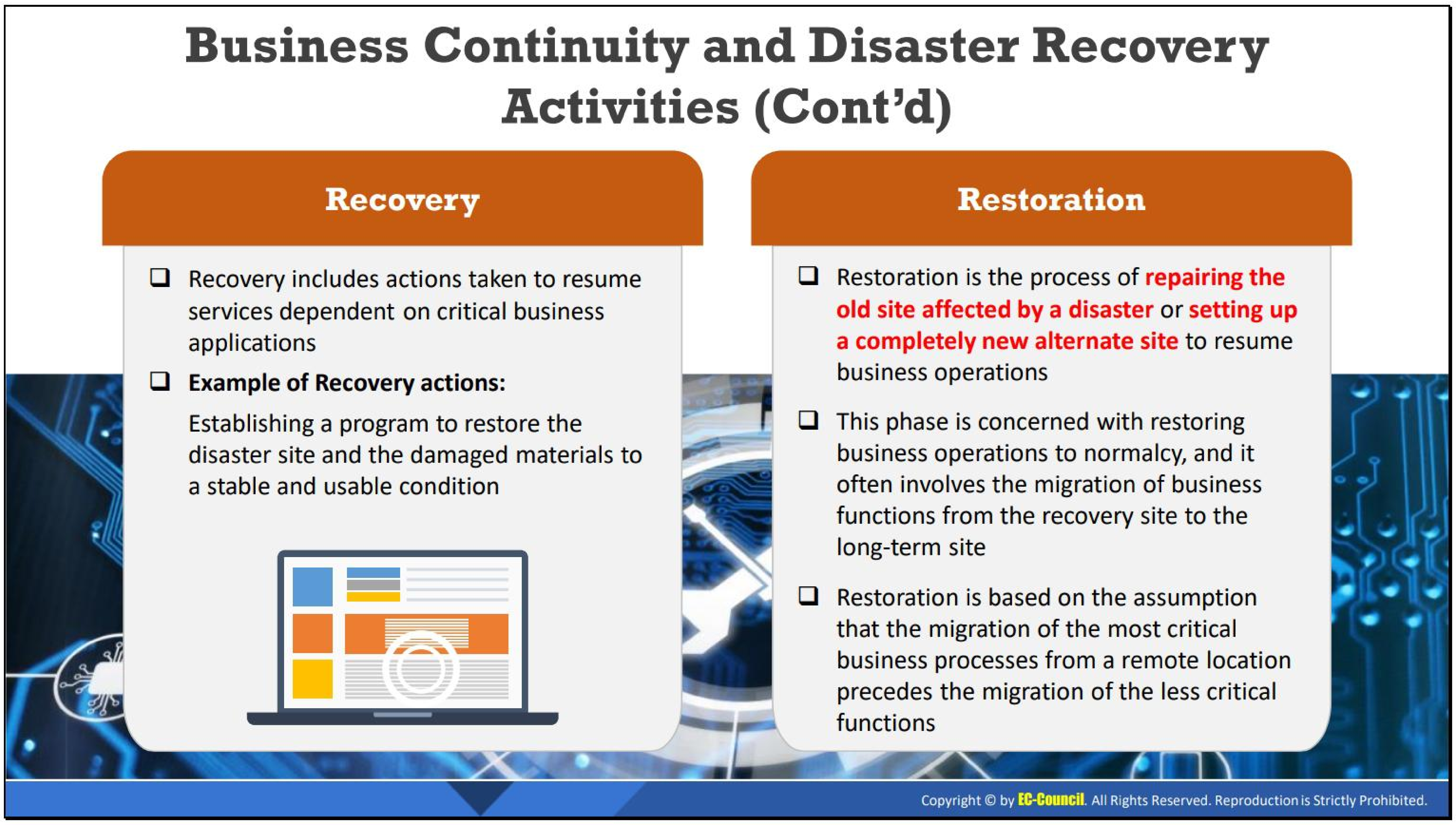
- ❑ In this process, **a set of activities are implemented** after a disaster in order to assess business needs and reduce and limit the negative impacts of the disaster
- ❑ **Example of response actions:**

  Evacuating personnel or shutting down systems

Resumption

- ❑ Resumption refers to the **recommencement of business operations** after a disruptive incident
- ❑ A robust organizational infrastructure is crucial to the execution of activities pertaining to resumption
- ❑ **Example of Resumption actions:**

  Continuing operations at a primary or an alternate operating location (an alternate site is used in case the primary location is inaccessible or unusable due to some reason)



Business Continuity and Disaster Recovery Activities (Cont'd)

Recovery

- ❑ Recovery includes actions taken to resume services dependent on critical business applications
- ❑ **Example of Recovery actions:**

  Establishing a program to restore the disaster site and the damaged materials to a stable and usable condition

Restoration

- ❑ Restoration is the process of **repairing the old site affected by a disaster** or **setting up a completely new alternate site** to resume business operations
- ❑ This phase is concerned with restoring business operations to normalcy, and it often involves the migration of business functions from the recovery site to the long-term site
- ❑ Restoration is based on the assumption that the migration of the most critical business processes from a remote location precedes the migration of the less critical functions

Business Continuity and Disaster Recovery Activities

The main BC and DR activities are prevention, response, resumption, recovery, and restoration.

- **Prevention**

  This activity involves actions taken to prevent a natural phenomenon or potential hazard from harming organizations. A preventive action is implemented concurrently and continuously along with certain proposed measures. It aims to reduce the likelihood and impact of a disruptive event and calls for deterrent and preventive control strategies. A deterrent control strategy minimizes the occurrence of threats, and a preventive control strategy protects critical business areas and mitigates the impact of a threat. In an effective prevention plan, prevention mechanisms do not allow unauthorized access or cause any availability problem. For example, these mechanisms restrict a company from spending money on certain processes not listed in the BCP and DRP.

- **Response**

  In this process, a set of activities are implemented after a disaster in order to assess business needs and reduce and limit the negative impacts of the disaster. For example, response actions include evacuating personnel or shutting down systems. An initial response includes the following:

  - Generating notifications
  - Activating the business continuity team (BCT)
  - Activating the business unit's personnel
  - Presenting an initial briefing to the BCT
  - Reviewing the recovery strategies for implementation
  - Implementing the BCP

- **Resumption**

  Resumption refers to the recommencement of business operations after a disruptive incident. A robust organizational infrastructure is crucial for executing the set of activities pertaining to resumption. An example of a resumption activity is continuing operations at a primary or an alternate operating location (an alternate site is used in case the primary location is inaccessible or unusable due to some reason). Resumption involves the activation of alternative infrastructure resources for facilitating smooth operations.

  Although resumption activates the time-sensitive business processes after a disruption, it cannot resume the activities in the case of large-scale destruction. In such cases, after consulting with their emergency operations center, organizations consider whether to invoke the BCP. The first decision pertains to whether critical operations should be resumed at the primary operating location or shifted to an alternate site. If the normal site is damaged or access to that site is denied, then operations are shifted to an alternate site.

- **Recovery**

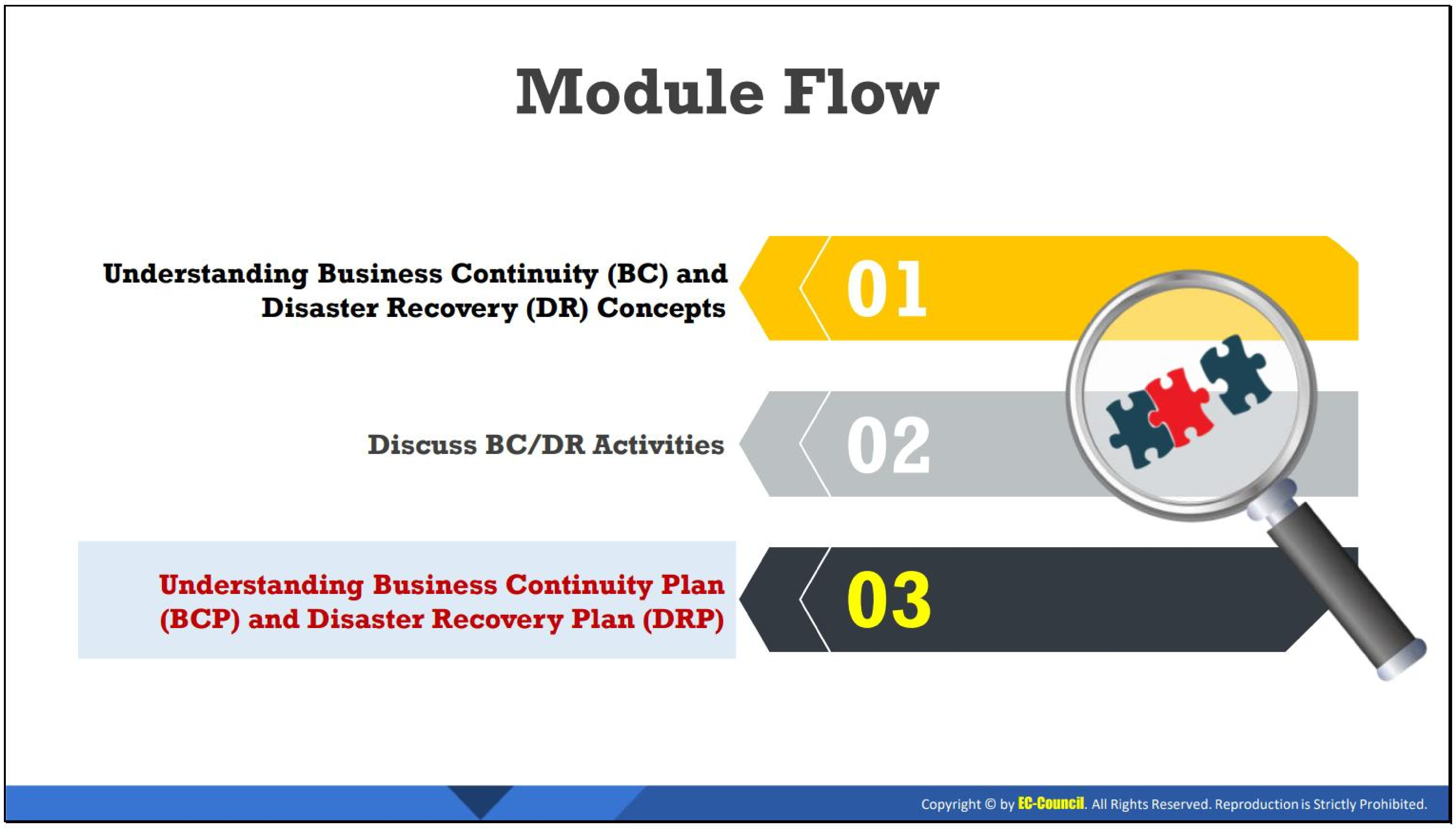
  Recovery includes actions taken to resume services dependent on critical business applications. An example of a recovery activity is establishing a program to restore both the disaster site and the damaged materials to the pre-disaster levels. It is a predetermined procedure of providing partial and temporary services to the unit affected by a disruption. Specifically, recovery focuses on a unit whose stakeholders are impacted by an interruption in the resumption of activities and a long restoration time. A recovery includes the following activities:

- Implementing recovery strategies
- Assessing damages in the primary facility
- Mobilizing the tactical teams for recovery
- Monitoring the recovery status
- Initiating the restoration process

- **Restoration**

  Restoration is the process of repairing the old site affected by a disaster or setting up a completely new alternate site to resume business operations. This process is concerned with the repair and restoration of the primary site. This phase is initiated only in the case of a physical damage. This phase is concerned with restoring business operations to normalcy, and it often involves the migration of business functions from the recovery site to the long-term site. In this phase, a team assesses the physical damage, replaces damaged items, and refurbishes the premises, thereby restoring normalcy to the operations. Restoration is based on the assumption that the migration of the most critical business processes from a remote location precedes the migration of the less critical functions.

  Initially, the operations team implements a DRP/BCP at the alternate site. Subsequently, the technical team formulates the restoration plan. The operations team is divided into two groups— one group continuously implements the DRP/BCP, and the other group manages the restoration process at the primary site. Often, the team simultaneously executes the restoration plan and the DRP/BCP.



Module Flow

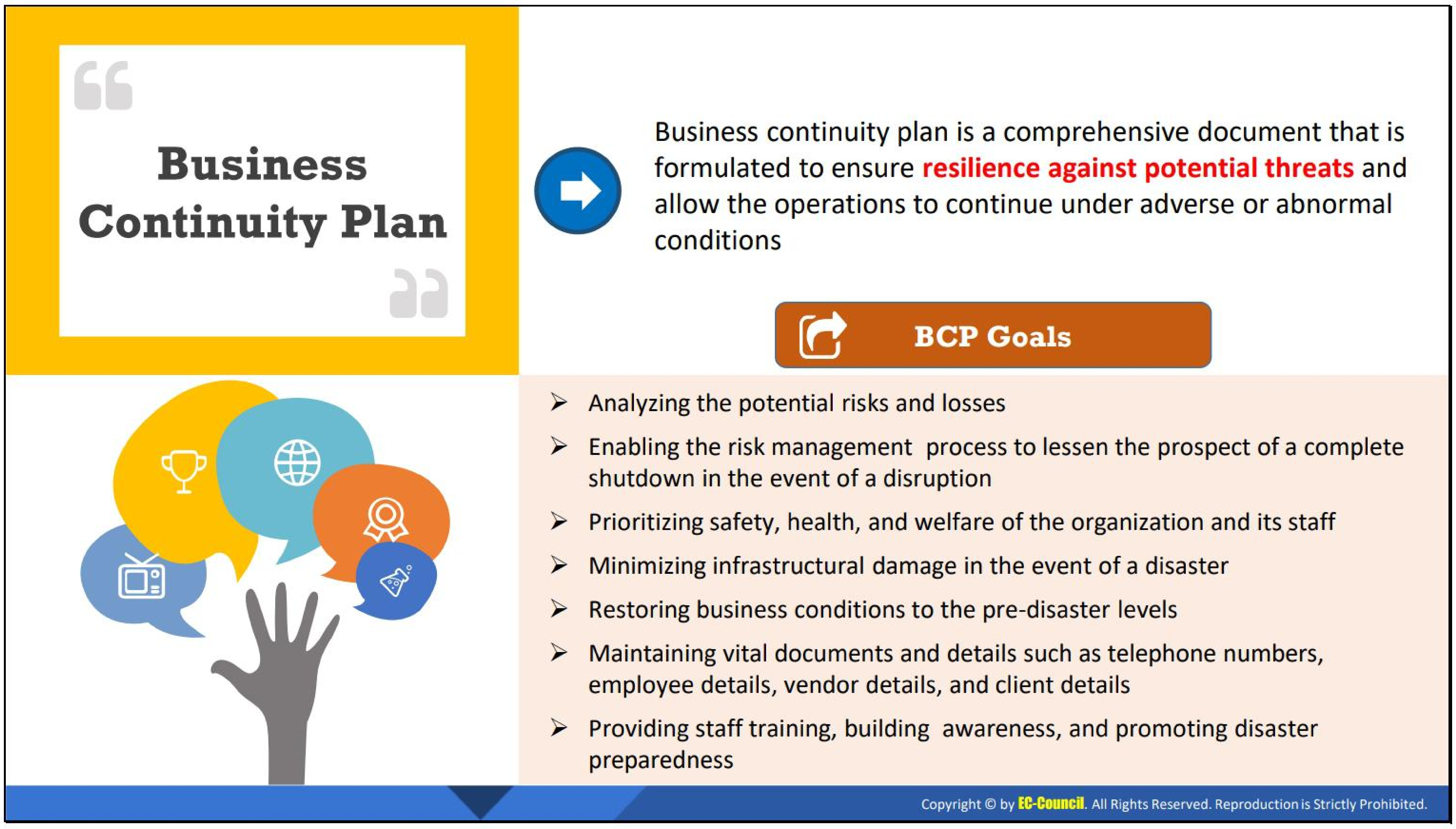
Understanding Business Continuity (BC) and Disaster Recovery (DR) Concepts 01

Discuss BC/DR Activities 02

Understanding Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) 03

Understanding Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

The objective of this section is to explain the BCP and the DRP and their goals.



Business Continuity Plan

Business continuity plan is a comprehensive document that is formulated to ensure **resilience against potential threats** and allow the operations to continue under adverse or abnormal conditions

BCP Goals

- Analyzing the potential risks and losses
- Enabling the risk management process to lessen the prospect of a complete shutdown in the event of a disruption
- Prioritizing safety, health, and welfare of the organization and its staff
- Minimizing infrastructural damage in the event of a disaster
- Restoring business conditions to the pre-disaster levels
- Maintaining vital documents and details such as telephone numbers, employee details, vendor details, and client details
- Providing staff training, building awareness, and promoting disaster preparedness

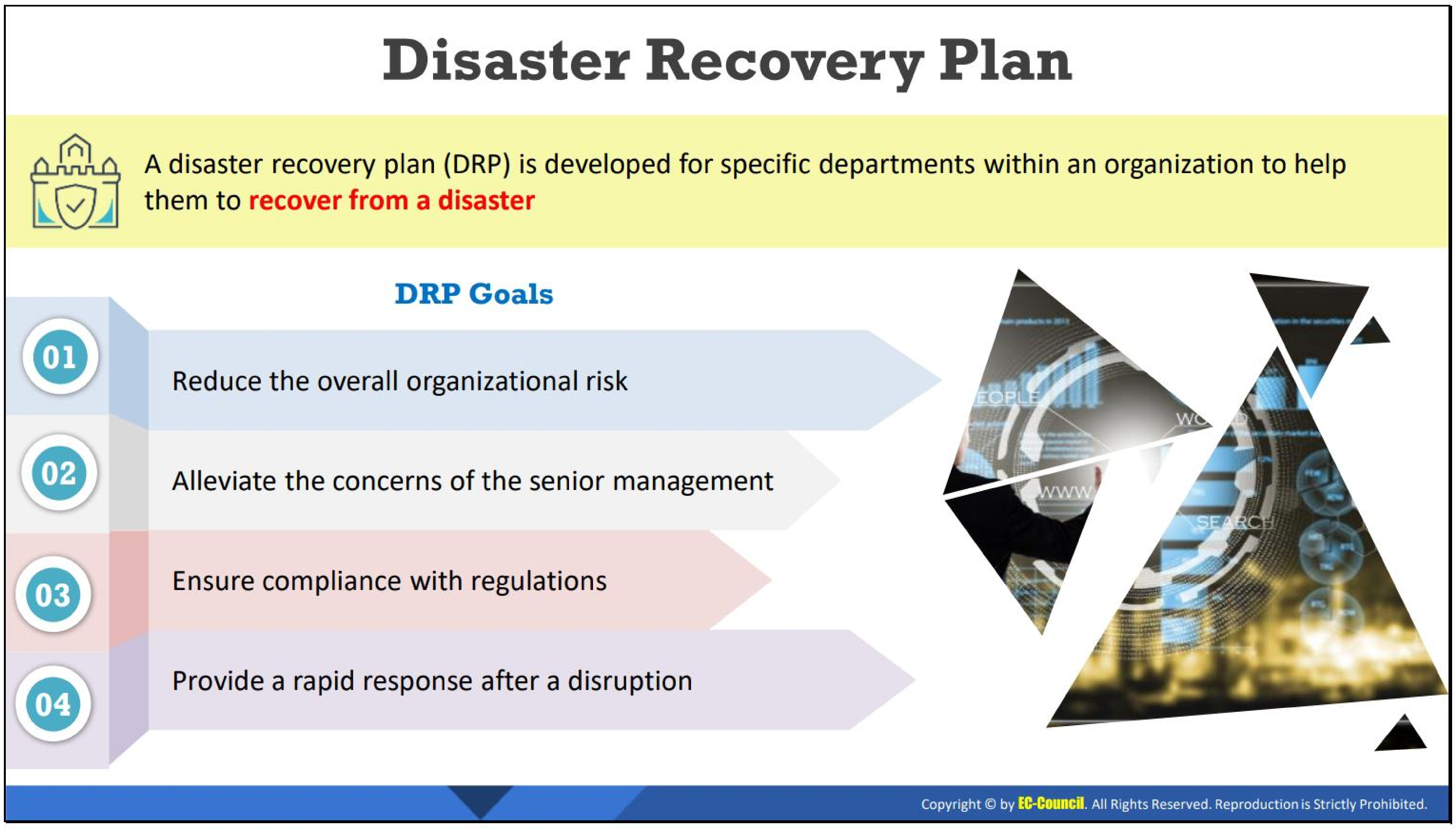
Business Continuity Plan

Business continuity plan is a comprehensive document that is formulated to ensure resilience against potential threats and allow the operations to continue under adverse or abnormal conditions. During a disruption, a BCP protects the personnel and assets of an organization. It is created using the inputs provided by several stakeholders.

Goals of a BCP

- **Analyzing the potential risks and losses:** Based on an analysis of the potential risks that can impact a business, a BCP contributes toward the formulation of continuity and recovery strategies. It also estimates the financial losses that may occur because of an interruption to critical business functions.
- **Enabling the risk management process:** A BCP aims to lessen the prospect of a complete shutdown because of a disruption. It guides an organization in its endeavor to recover from and prevent a disaster while reducing the risks of an operational downtime. It predicts the likelihood of events that disrupt organizational operations, determines the extent of disruption, and provides preventive measures to mitigate their effects.
- **Prioritizing safety, health, and welfare of the organization and its staff**: The incident response plan of a BCP regulates the impact of a disruption through a set of responses such as an evacuation, emergency health services, and personnel safety and welfare.
- **Minimizing infrastructural damage in the event of a disaster:** A proper BCP ensures minimal damage to the IT infrastructure during an incident.

- **Restoring business conditions to the pre-disaster levels:** A BCP reduces the impact of a disaster and contributes toward restoring business operations within a short time.
- **Maintaining vital documents and details:** As part of the BCP, an organization maintains a list of important details such as telephone numbers, employee details, vendor details, and client details. During an emergency, these details help an organization to establish contact with emergency services, vendors, and media. It controls the spread of negative information and provides assurance to affected stakeholders. Specifically, a BCP facilitates the implementation of a pre-defined communication plan to address all requirements.
- **Providing staff training, building awareness, and promoting disaster preparedness:** An organization must ensure that its employees are aware of its BCP; this is crucial to the successful implementation of a BCP. Employees should receive proper training on the types and purposes of BCPs and the objectives of BCP implementation during a disruption. An organization must also be aware of its employees’ expectations during a disruption.



Disaster Recovery Plan

A disaster recovery plan (DRP) is developed for specific departments within an organization to help them to **recover from a disaster**

DRP Goals

01 Reduce the overall organizational risk

02 Alleviate the concerns of the senior management

03 Ensure compliance with regulations

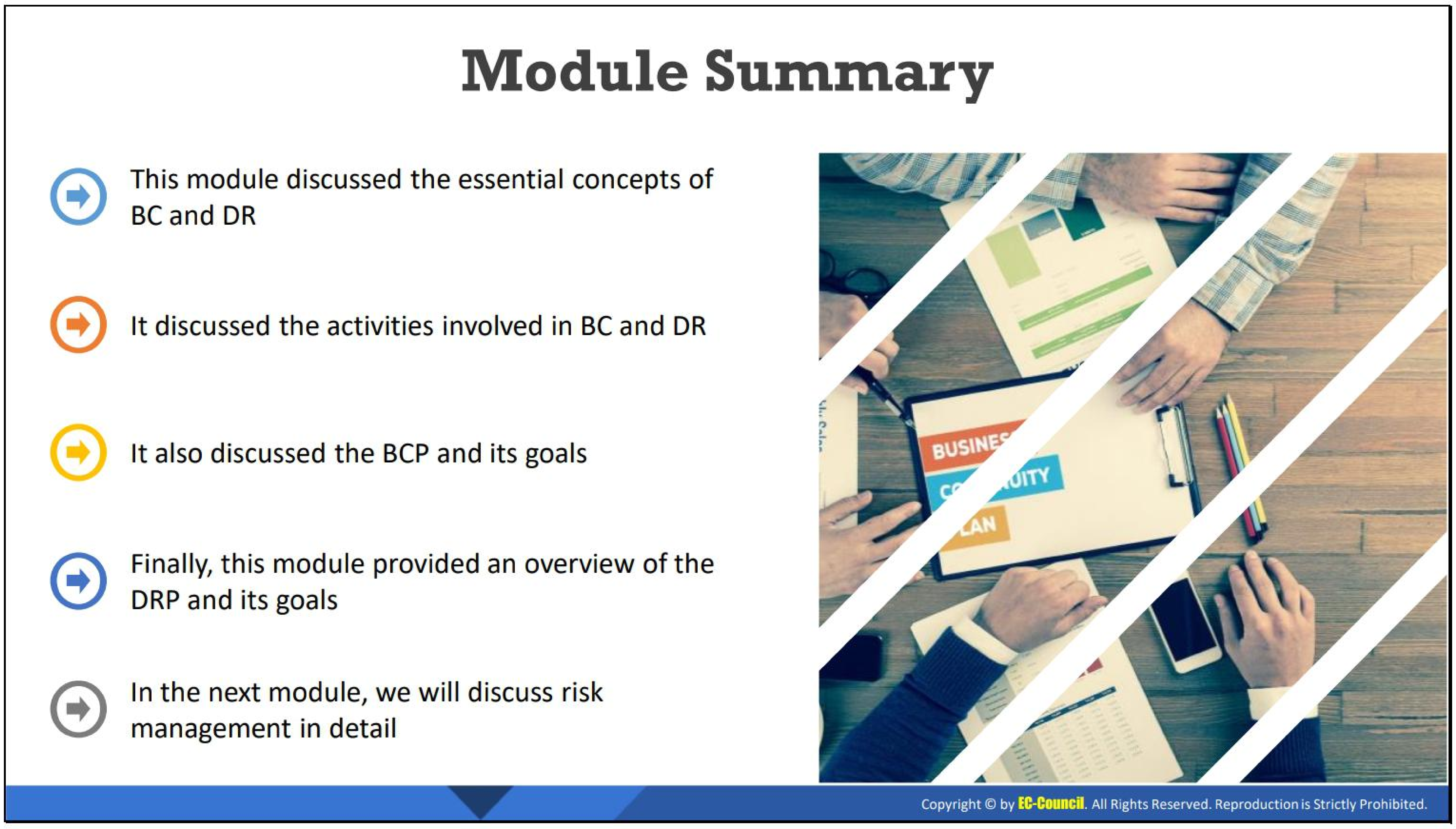
04 Provide a rapid response after a disruption

Disaster Recovery Plan

A disaster recovery plan (DRP) is developed for specific departments within an organization to help them to recover from a disaster. It elaborates on the preventive mechanisms an organization must adopt to reduce the effects of the disaster in order to continue or instantaneously resume critical business functions.

Goals of a DRP

- **Reduce the overall organizational risk:** A DRP reduces the likelihood and the impact of a risk and increases the resilience of business operations. A good DRP aims to minimize an organization's overall risk. Therefore, before formulating a DRP, companies must conduct a risk assessment to identify critical vulnerabilities.
- **Alleviate the concerns of the senior management:** A DRP is an important part of an operations strategy, and its success is determined by the support received from the senior management. Hence, the goals and scope of a DRP must align with the expectations of the senior management. After formulation, the DRP should be submitted to the senior management for their approval. An approved not only alleviates senior management's concerns but also ensures its smooth implementation and enforcement.
- **Ensure compliance with regulations:** Most organizations uphold the various compliance standards. An effective DRP minimizes the chance of penalties as a result of a non-compliance.
- **Provide a rapid response after a disruption:** Since a disaster causes customer dissatisfaction, revenue loss, and reputational damage, it is crucial for a DRP to provide a quick response in the event of a disruption. A good DRP contributes toward expediting a disaster response, irrespective of the source of disruption.



Module Summary

- This module discussed the essential concepts of BC and DR
- It discussed the activities involved in BC and DR
- It also discussed the BCP and its goals
- Finally, this module provided an overview of the DRP and its goals
- In the next module, we will discuss risk management in detail

BUSINES
UITY
LAN

Module Summary

This module discussed the essential concepts of BC and DR. It discussed the activities involved in BC and DR. It also discussed the BCP and its goals. Finally, this module provided an overview of the DRP and its goals.

In the next module, we will discuss risk management in detail.