EC-Council

Building A Culture Of Security

C|ND

Certified Network Defender

Certified Network Defender v3

MODULE 17

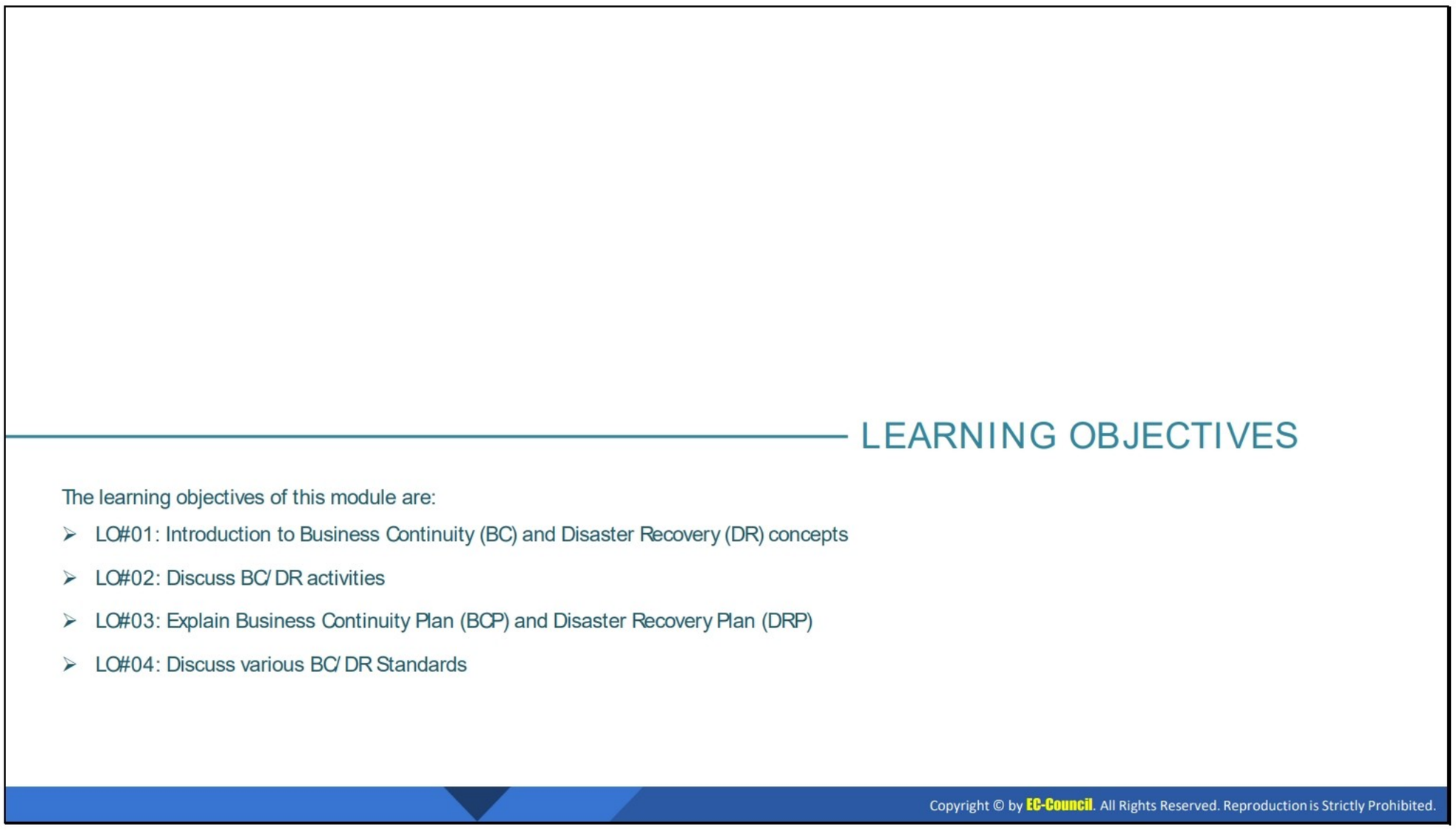
BUSINESS CONTINUITY AND DISASTER RECOVERY

EC-Council Official Curricula

https://t.me/learningnets

This page is intentionally left blank.

https://t.me/learningnets



Learning Objectives

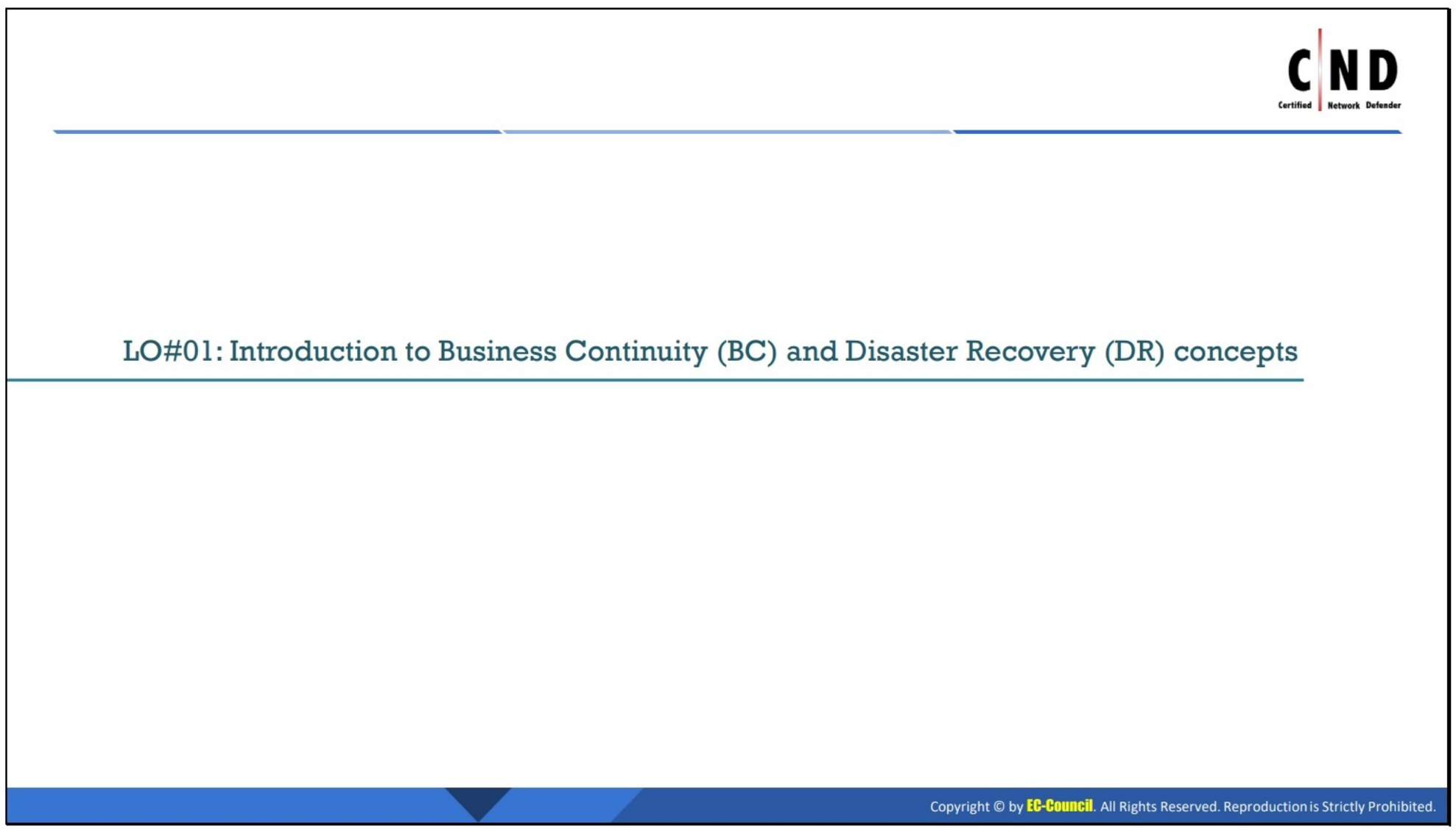
When threatened by a disruptive event, organizations should be capable of minimizing its impact, ensuring business continuity, and accelerating the disaster recovery process. As key personnel of an organization, network defenders should be well-acquainted with their organization's business continuity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

The learning objectives of this module are to:

- Business Continuity (BC) and Disaster Recovery (DR)
- BC/DR activities
- Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
- Standards of BC/DR

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

https://t.me/learningnets

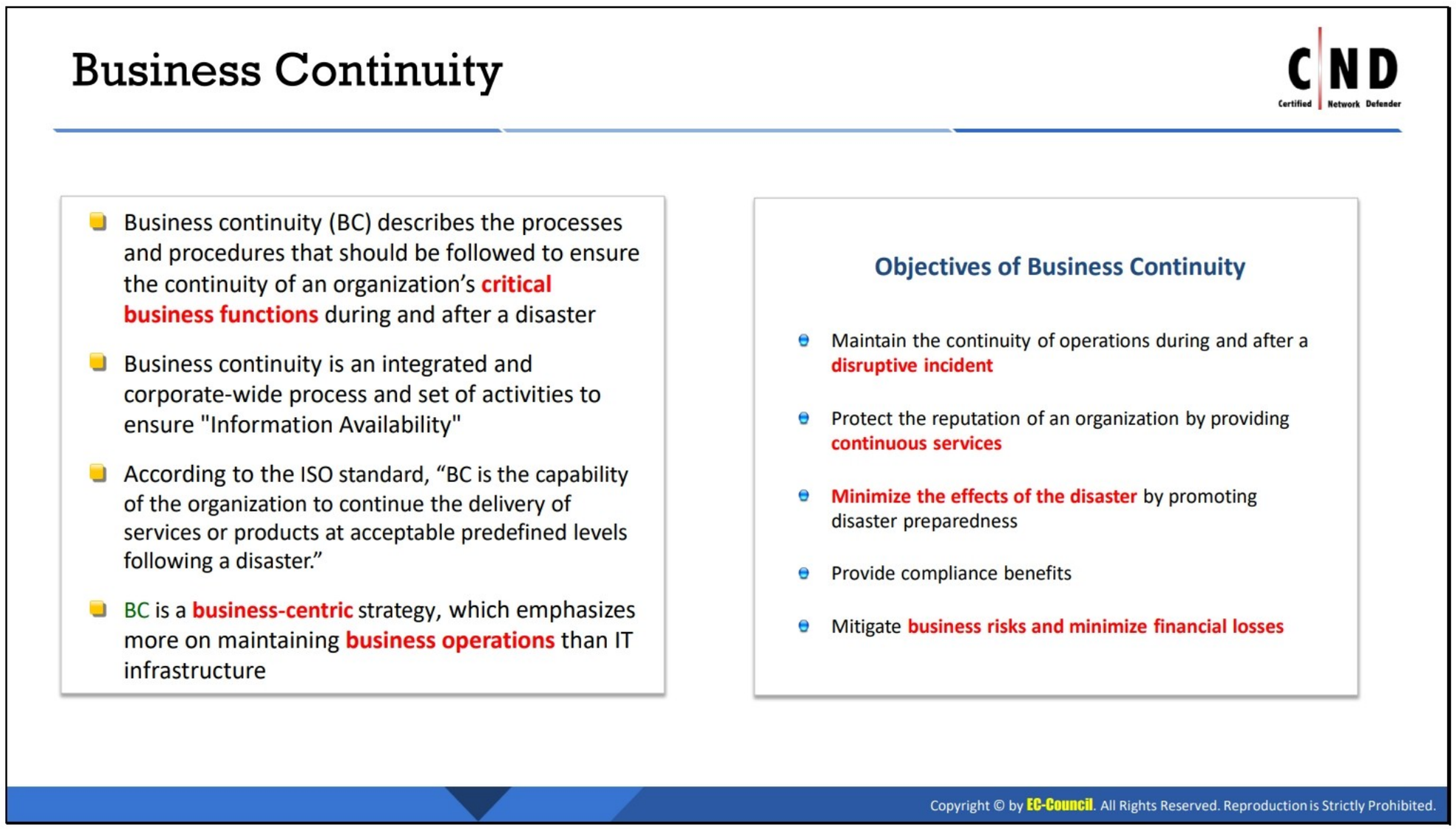


LO#01: Business Continuity (BC) and Disaster Recovery (DR) Concepts

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).

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

https://t.me/learningnets



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." It is a comprehensive, enterprise-wide process designed to ensure the seamless continuation of activities across various environments. It aims to guarantee uninterrupted information availability through a coordinated set of actions.

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.

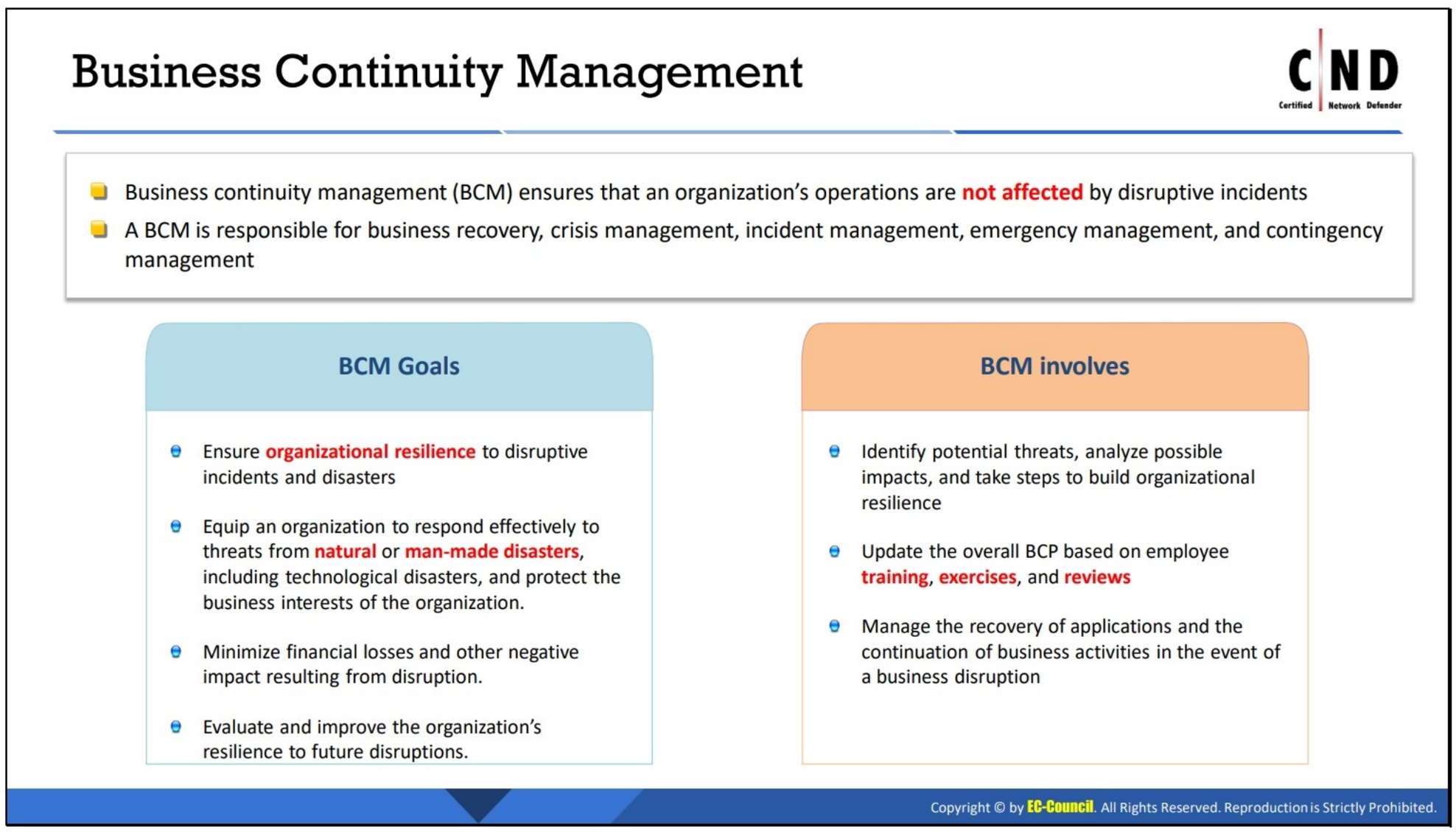
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **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.

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

https://t.me/learningnets



Business Continuity Management

Business continuity management (BCM) is a process that ensures the continuity of business operations after disruptive incidents. 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 (IcM) 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.

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

https://t.me/learningnets

- **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

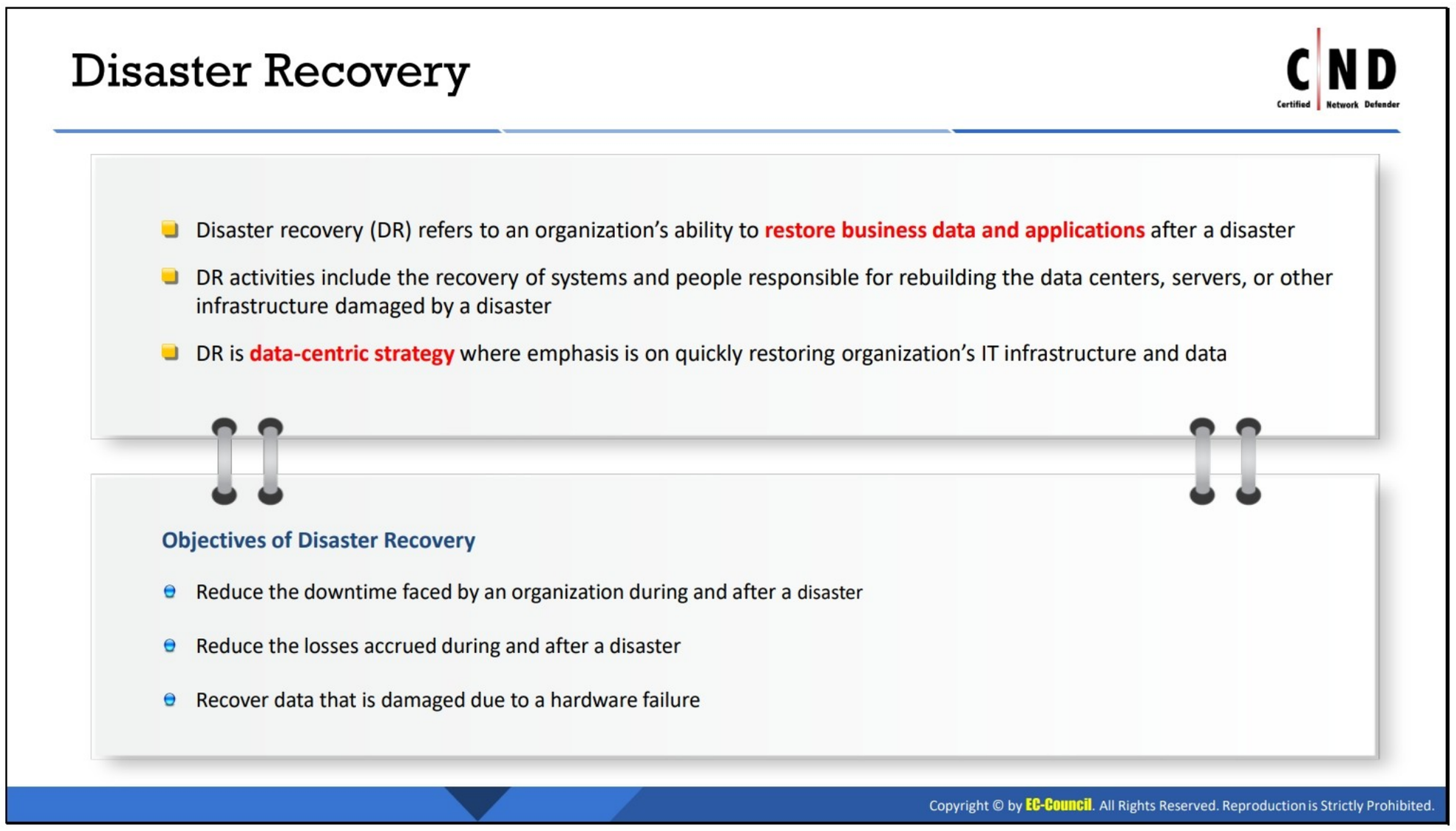
- **Ensure organizational resilience to disruptive incidents and disasters:** The security requirements of an organization can be ascertained through a business impact analysis and CM, DRP, and BCP. These plans should motivate employees to contribute collectively toward improving their organization's 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.
- **Minimize financial losses:** Financial losses in the event of disruptions and disasters are minimized.
- **Evaluation:** Evaluation can improve reliability and resilience to any operational disruptions in future. Consistent documents reviews and mock drills can strengthen the organization to minimize vulnerabilities and so business continuity.

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.

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

https://t.me/learningnets



Disaster Recovery

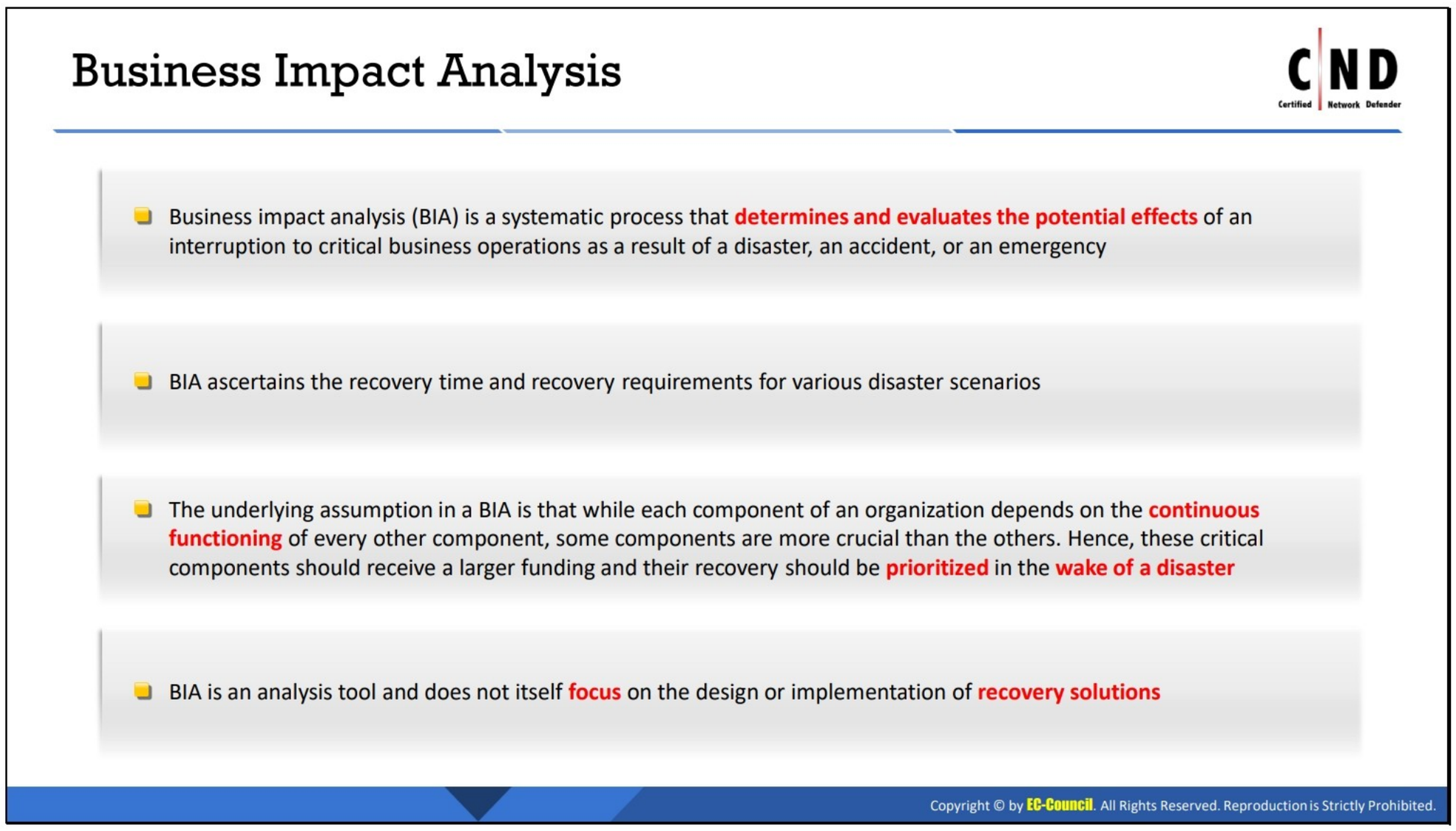
Careful security planning contributes toward mitigating the impact of disasters on organizations. Disaster recovery (DR) is an area of security planning that reflects an organization's ability to restore business data and applications after a disaster. It involves a set of procedures and policies aimed 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.

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

https://t.me/learningnets



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.

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

https://t.me/learningnets

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.

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

https://t.me/learningnets

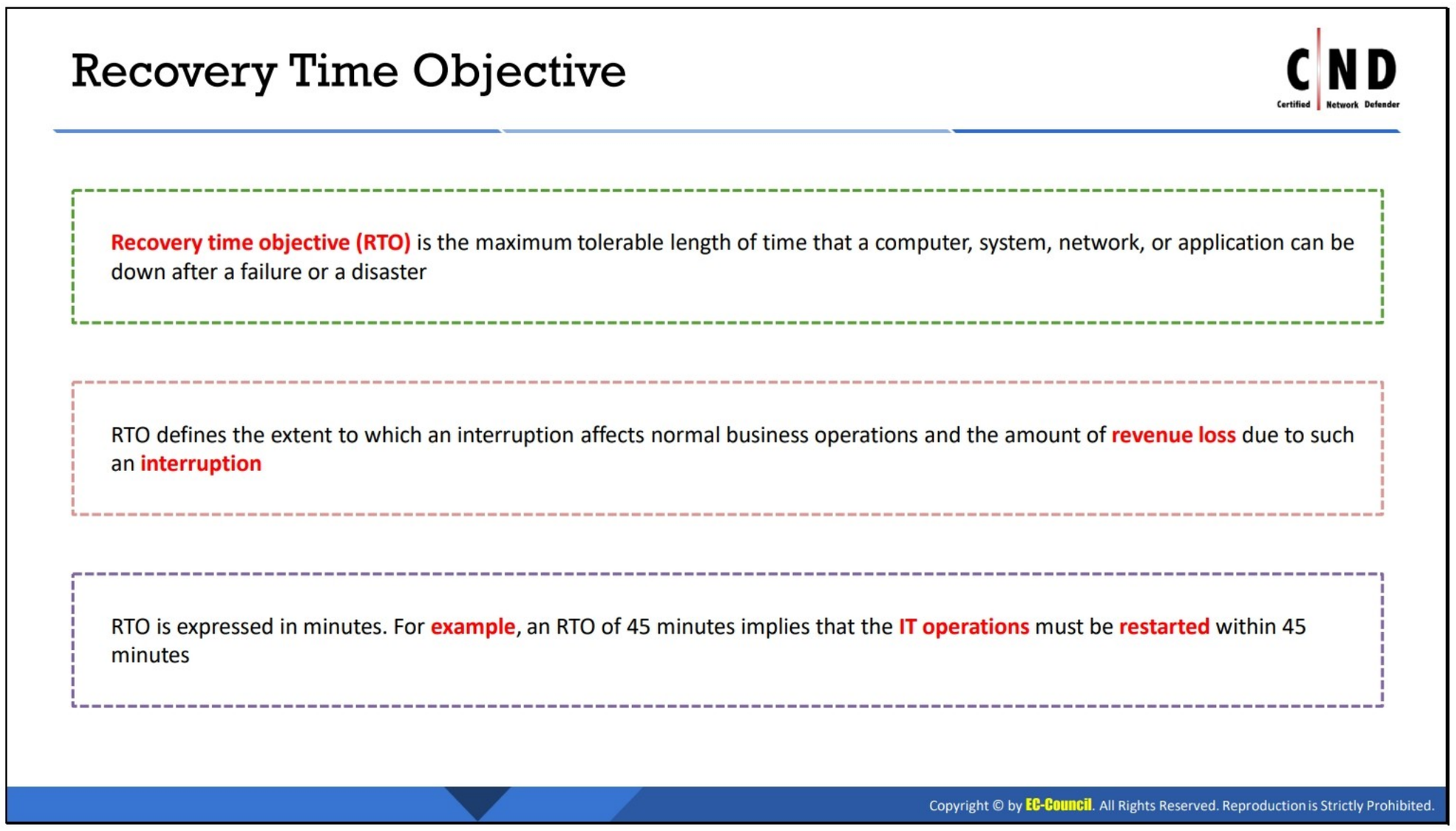
- **Phase 5: Presentation of the BIA Report to the Management**

  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.

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

https://t.me/learningnets



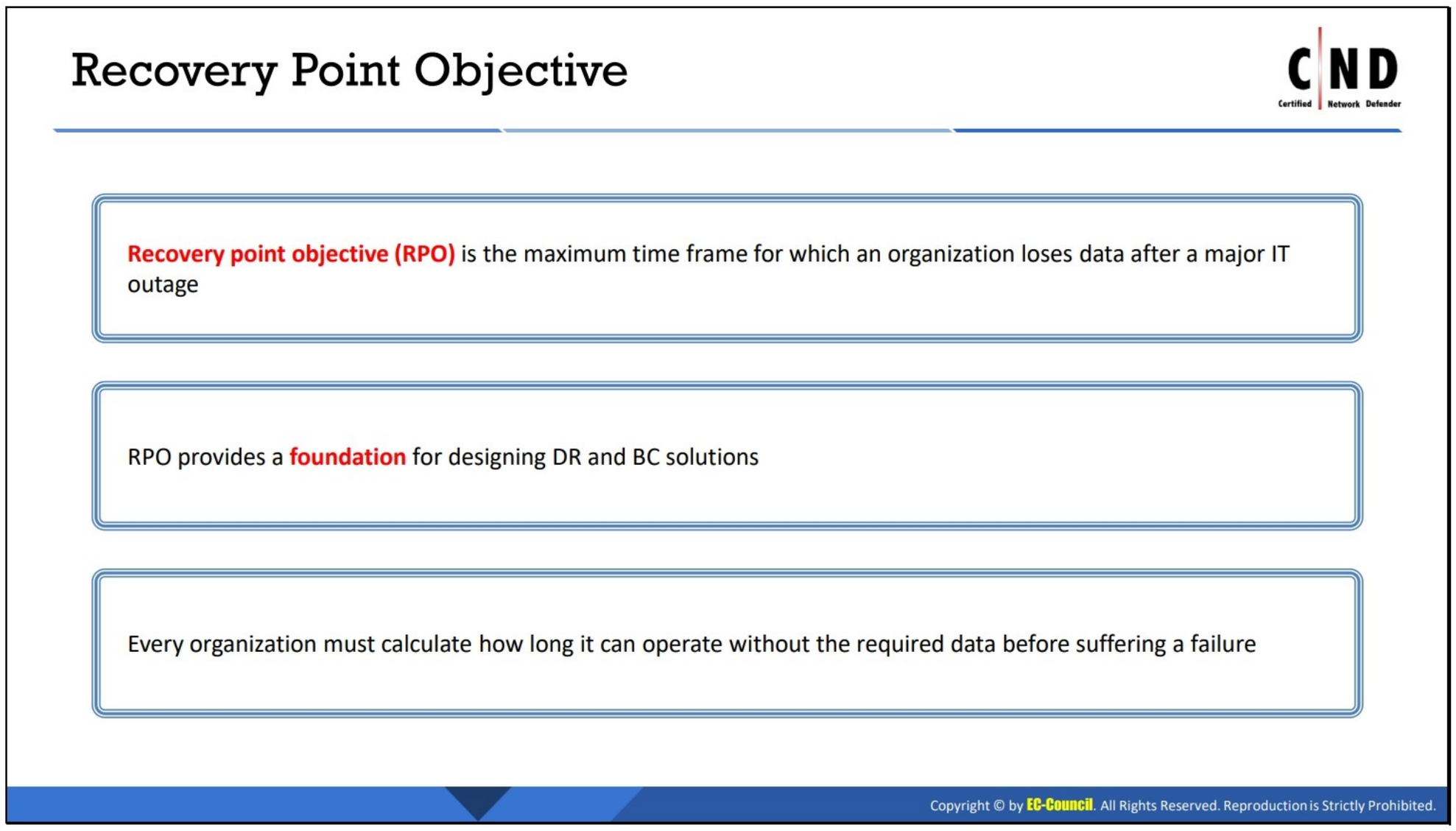
Recovery Time Objective

A recovery time objective (RTO) is defined as the maximum tolerable length of time a computer, a system, a network, or an application can be down after a failure or a disaster. Established by the process owner during the BIA, an RTO is a metric that calculates how fast an organization recovers its services and the IT infrastructure following a disaster event. In other words, it measures the time an organization takes to return to its pre-disaster operational levels. It is measured in seconds, minutes, hours, or days. An RTO of 45 minutes means that an organization can maintain operations for that period after the disruption of its infrastructure and the resulting data loss. If the organization fails to restore the infrastructure and data within the RTO of 45 minutes, then the business may suffer an irreparable loss. Given this, an RTO determines the extent to which the disaster interrupts the normal operations and the resulting loss of revenue per unit time, and hence it is crucial to DRP. These factors entirely depend on the affected application(s) and the equipment(s).

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 network defender 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).

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

https://t.me/learningnets



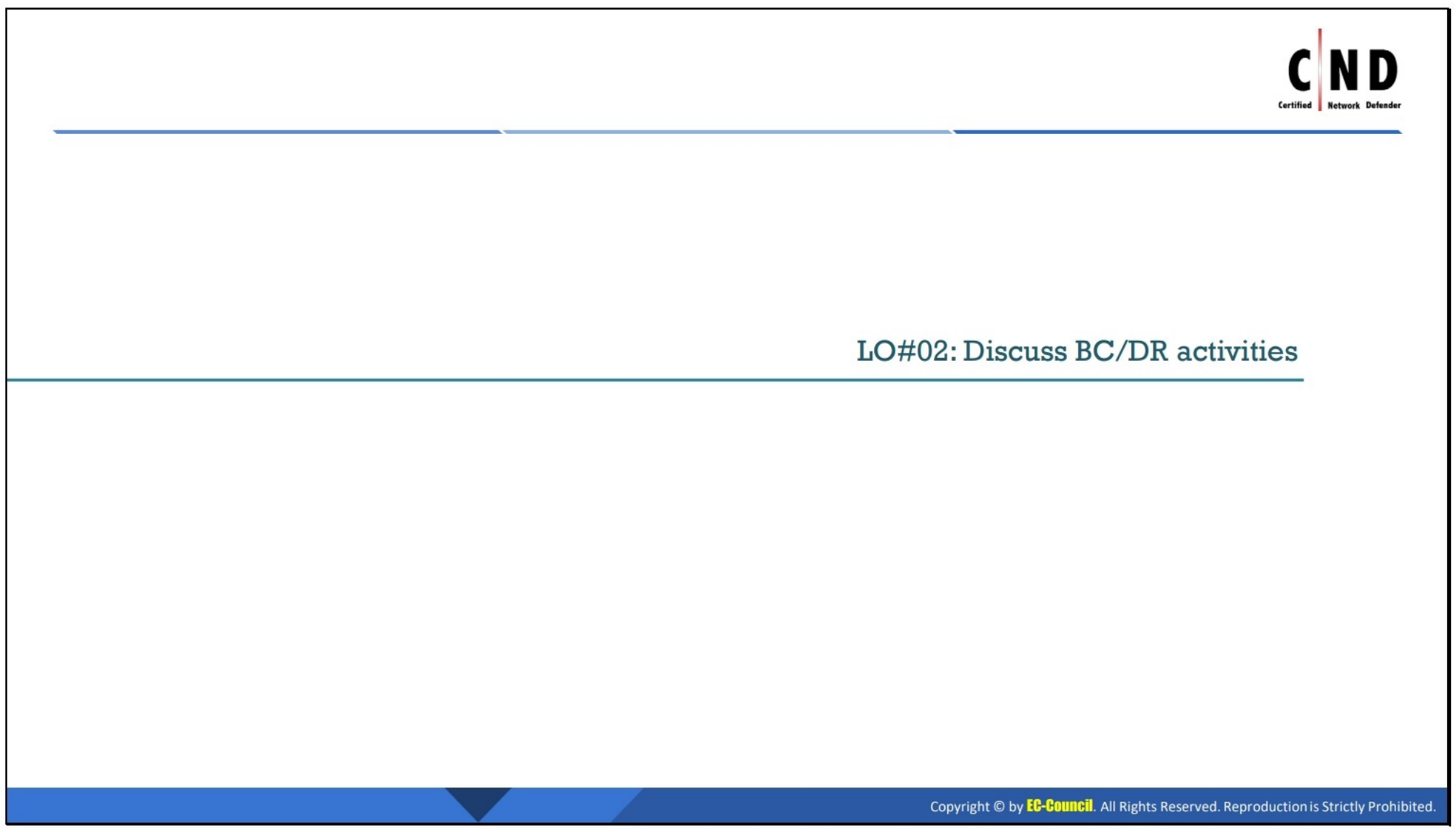
Recovery Point Objective

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 network defender 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).

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

https://t.me/learningnets

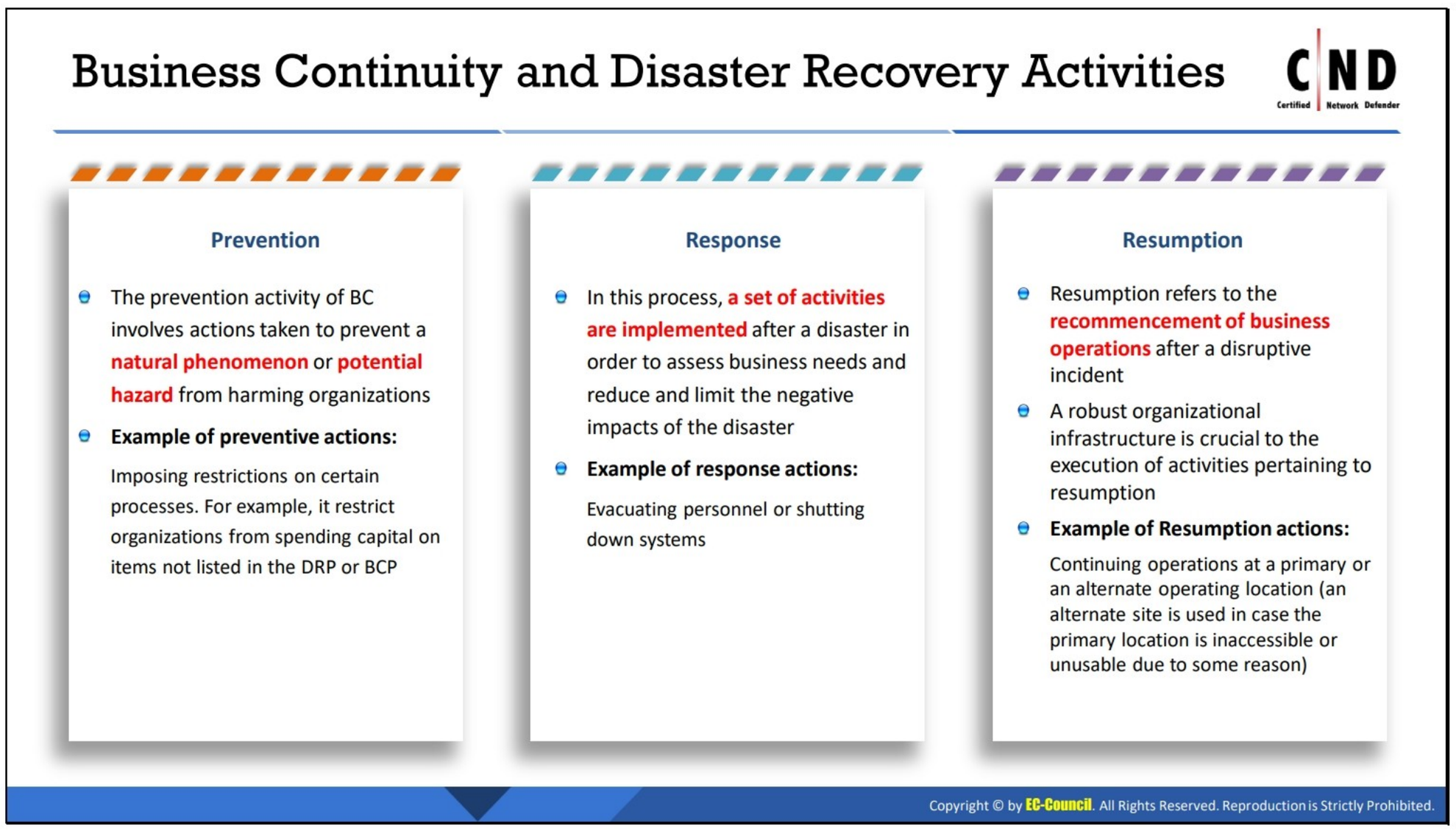


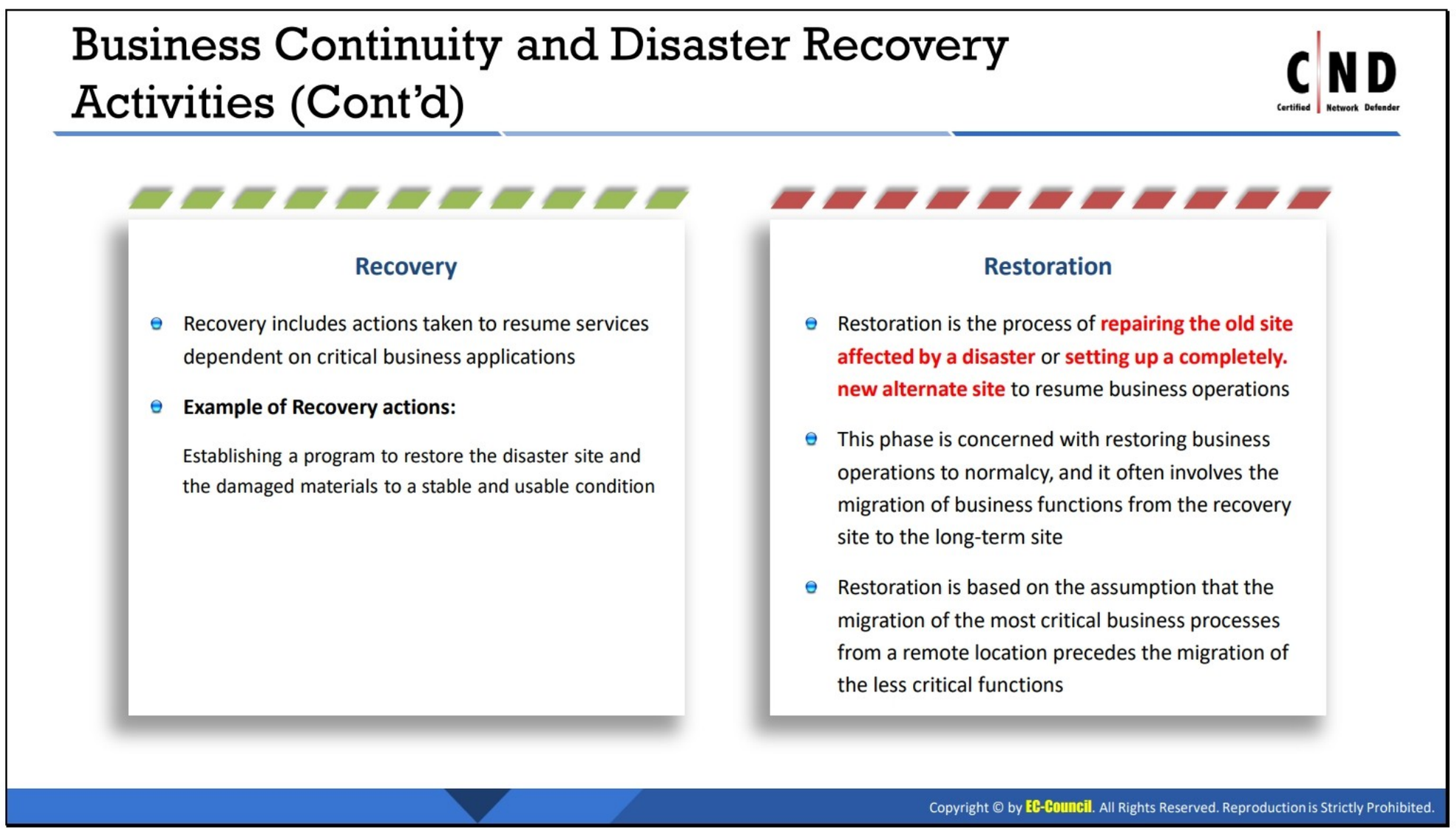
LO#02: Discuss BC/DR Activities

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.

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

https://t.me/learningnets





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

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

https://t.me/learningnets

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. 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

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

https://t.me/learningnets

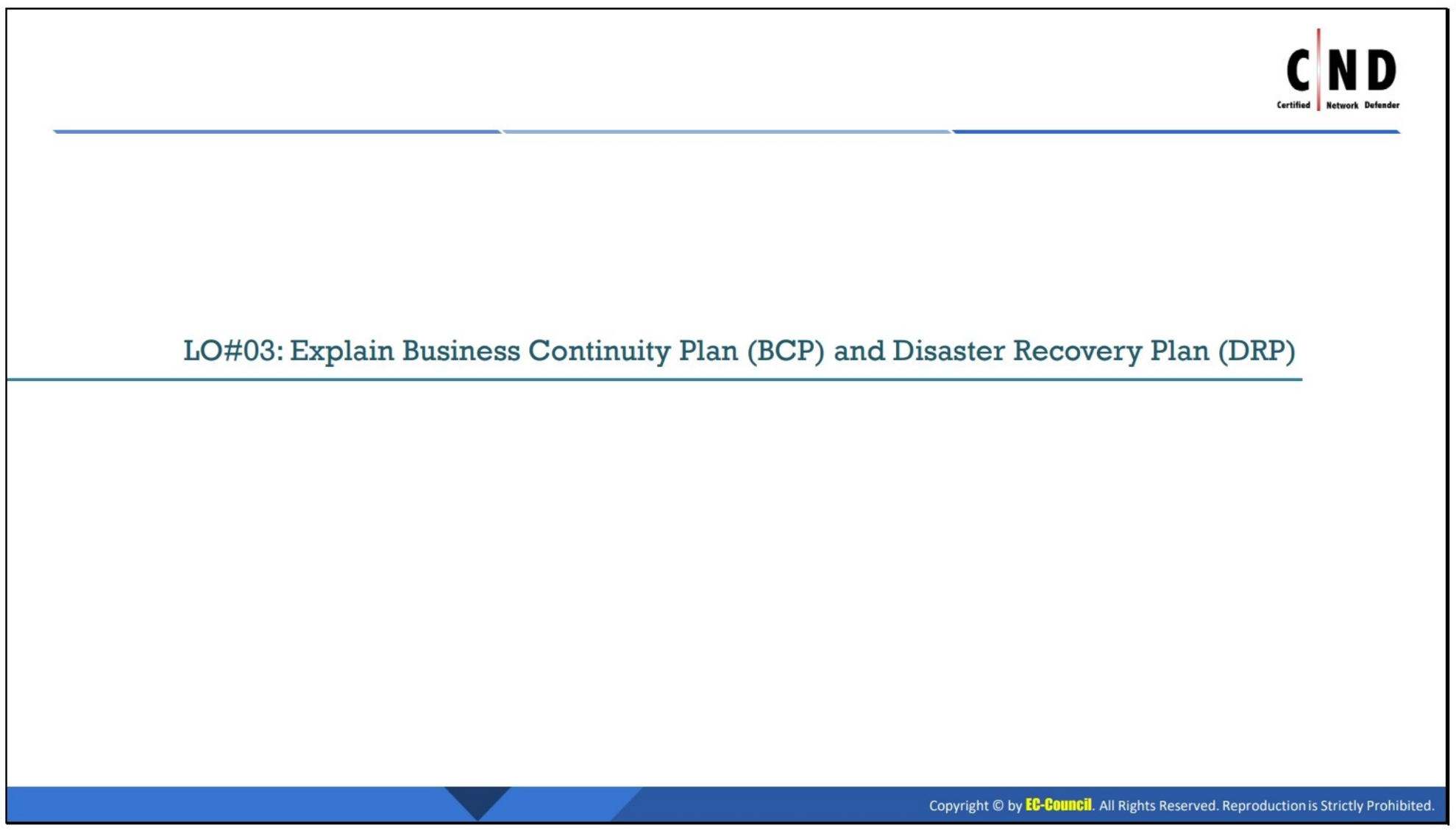
Restoration

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. In this phase, a team assesses the physical damage, replaces damaged items, and refurbishes the premises, thereby restoring normalcy to the operations.

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.

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

https://t.me/learningnets

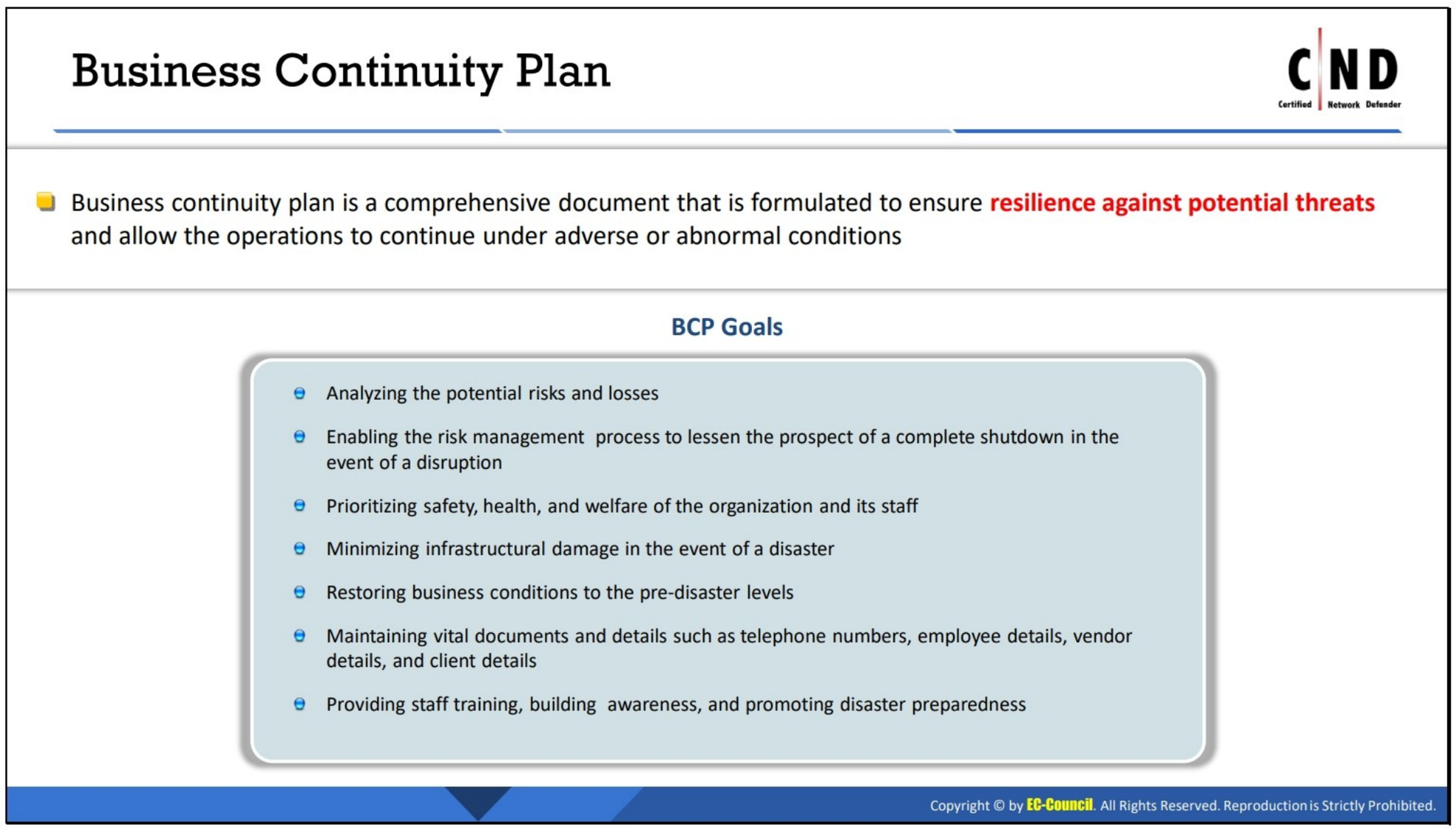


LO#03: Explain Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

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

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

https://t.me/learningnets



Business Continuity Plan

A BCP is prepared to help an organization develop resilience to potential threats, and thereby ensure BC. 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.
- **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

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

https://t.me/learningnets

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.

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

https://t.me/learningnets

Disaster Recovery Plan

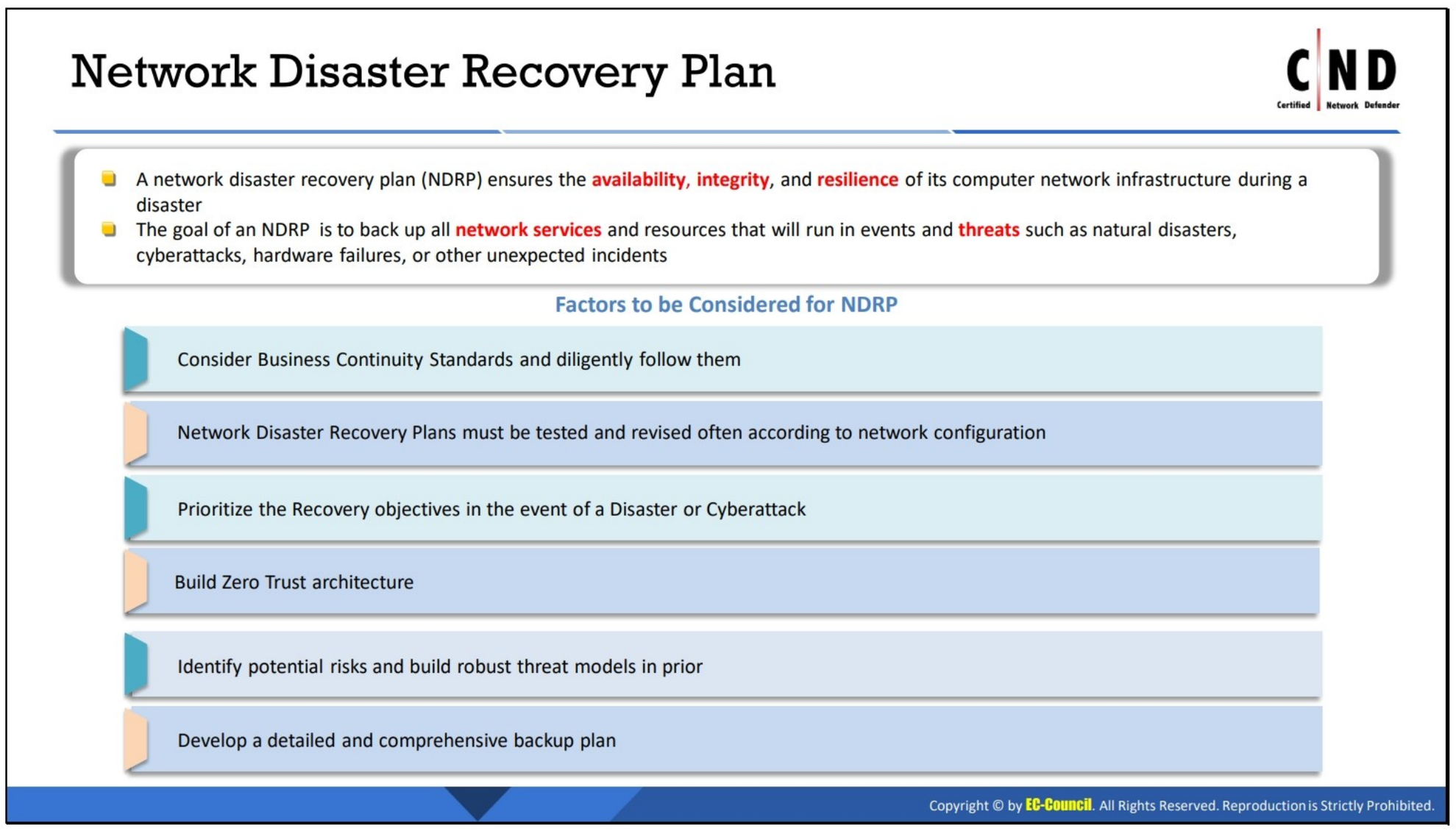
A DRP is developed to respond to an unexpected disruptive event (to recover from a disaster). It elaborates on the preventive mechanisms an organization must adopt to reduce the effects of the disaster in order to continue or instantaneously resume critical business functions.

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.

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

https://t.me/learningnets



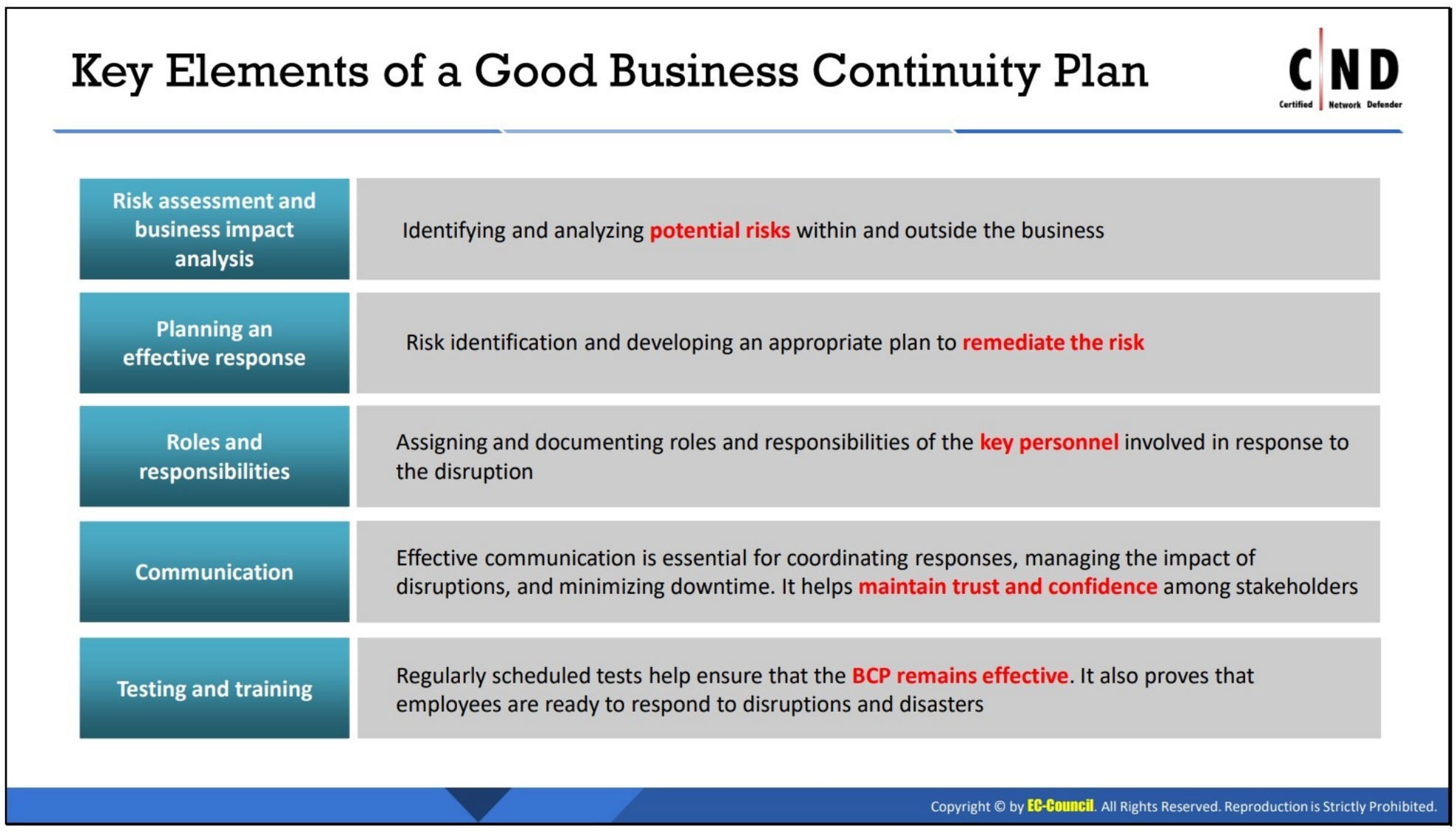
Network Disaster Recovery Plan

The factors to be considered with a network disaster recovery plan are as follows:

- Follow Business Continuity disaster recovery standards, as they provide an appropriate foundation to build contingency plans.
- Network disaster recovery plan needs to be evaluated frequently to make sure they consider changes to the network, personnel, possible risks, and organizational business goals.
- The organization must decide on its recovery time goal (RTO) and recovery point objective (RPO) for each essential service and data type before developing a strategy.
- Zero-trust architecture features a security structure that implies no implicit trust, continually inspects and monitors network operations, and applies strict access restrictions, which is vital for network disaster recovery.
- Potential external threats might also be a big concern when recuperating after an incident. Damage from malicious actors such as hackers or malware could extend beyond regular system failure or hardware problems.
- Backup data to specialized backup disk appliances using management software, either built into the appliance or running on a separate server.

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

https://t.me/learningnets



Key Elements of a Good Business Continuity Plan

The elements of a good Business Continuity plan are as follows:

- Assessing the risks that could potentially disrupt those business processes comes after you have determined which processes are essential to the corporation. This covers pandemics, cyberattacks, power disruptions, and natural calamities. Your ability to prioritize important business operations and develop a risk mitigation strategy will be aided by risk assessment.
- Recognizing potential disruptions and estimating the potential harm they could do to the resources impacted. For example, a power outage can potentially lead to the inability to access the servers, whereas a cyber-attack can result in data theft and network downtime.
- The actions that will be carried out to keep the organization operating in the event of an interruption are described in the business continuity strategy. The plan should consider every aspect of the business continuity plan, from employees and structures to procedures and technology, and should be specifically suited to the organization's needs.
- Data backups should be kept in several separate locations. This avoids simultaneous destruction of the original and backup copies. In addition, offline copies should be retained if necessary.
- Business impact analysis is a technique for locating and evaluating the possible effects of disruption to essential company operations. The organization can determine which business operations are essential to the organization's survival and which can be stopped without having a significant negative impact.

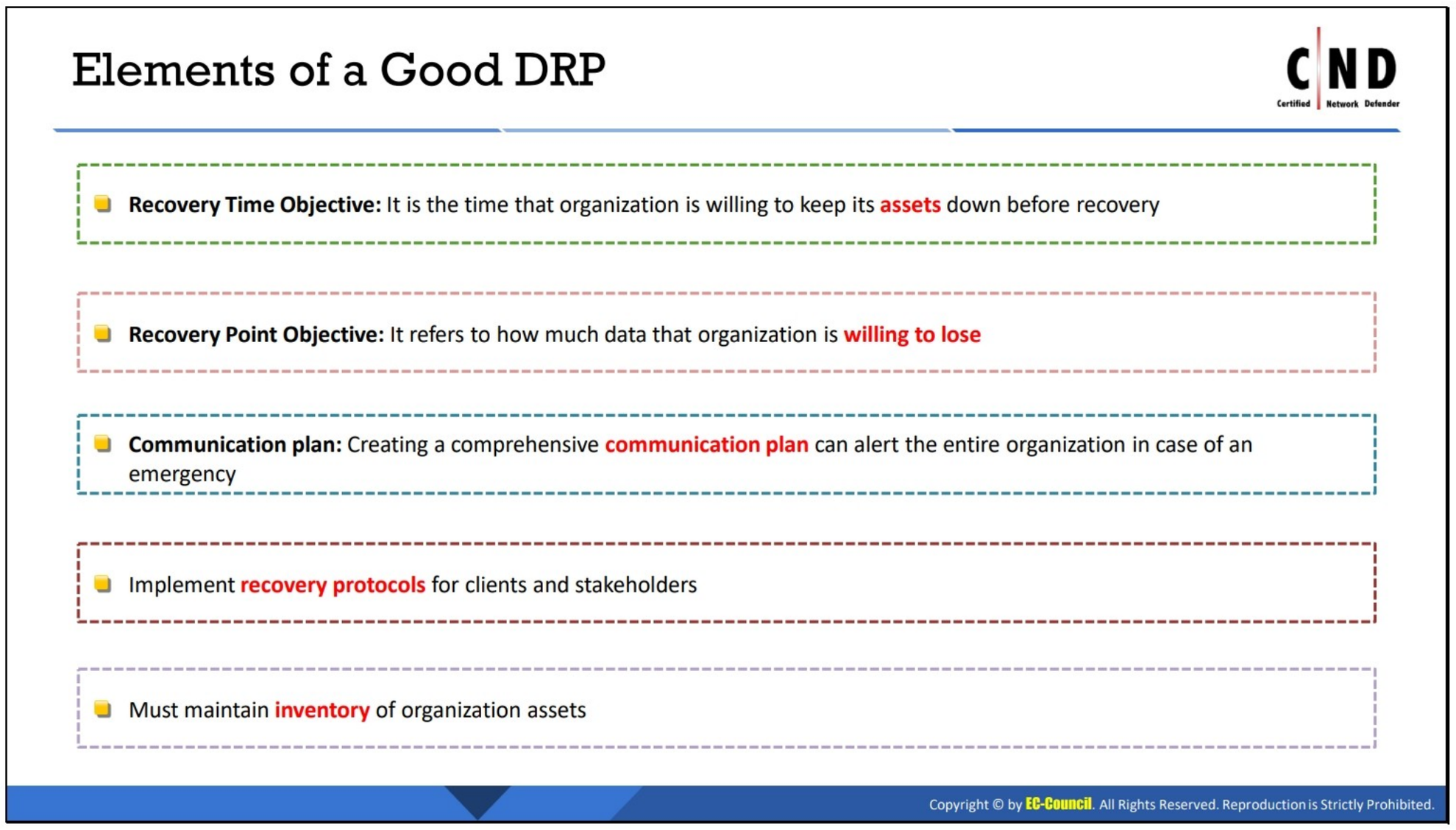
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- The technique a corporation uses to reduce its exposure to the many dangers it can encounter is known as risk mitigation. Organizations evidently deal with a variety of risks, some of which can result in significant disruption or monetary loss. A wise action that any business should take to prevent such unwanted consequences is mitigation.

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

https://t.me/learningnets



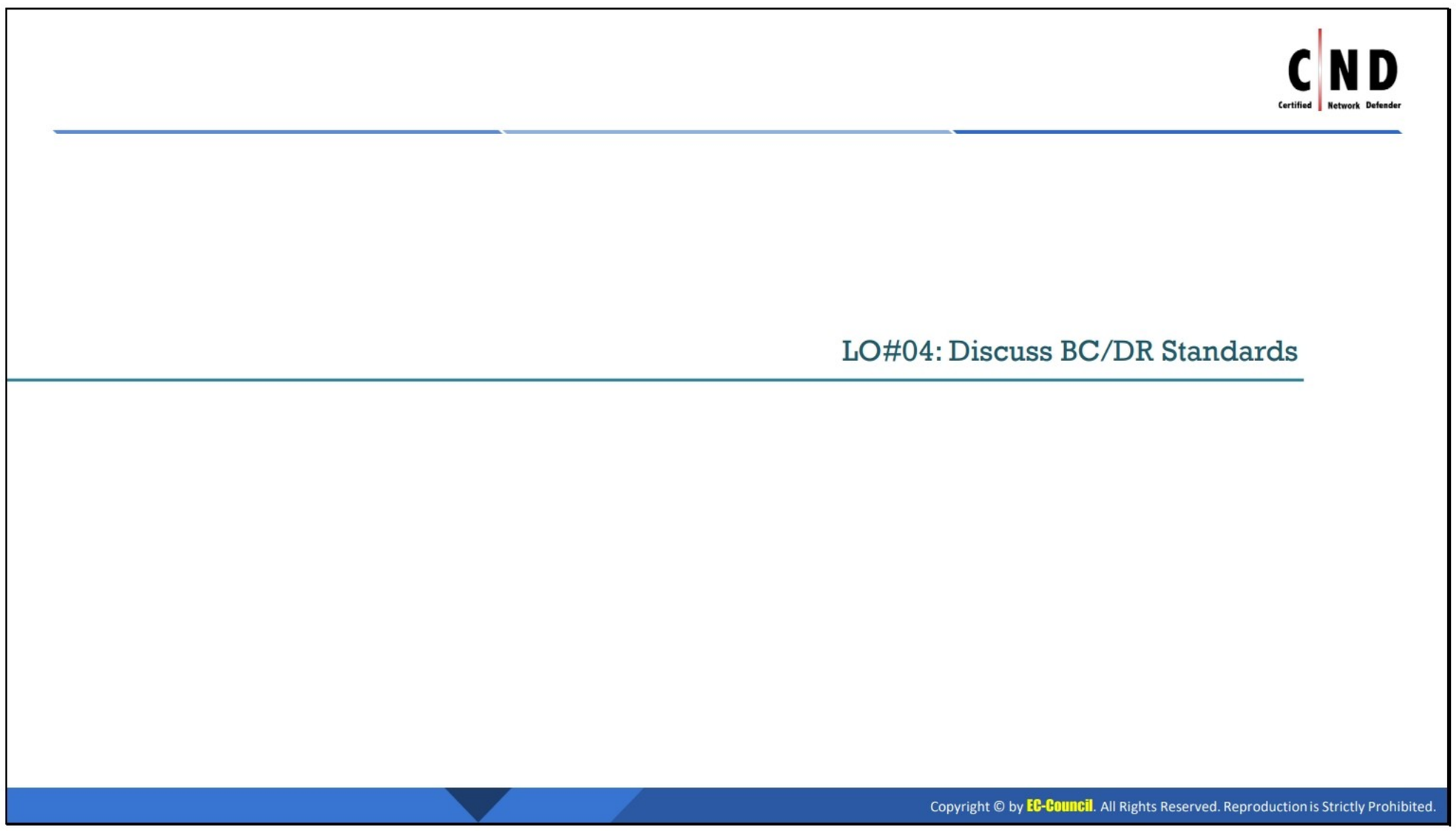
Elements of a Good DRP

The elements of a good Disaster Recovery Plan are listed below:

- The Recovery Time Objective (RTO) is the time limit determined for the restart of the organization and IT services following a disaster. The RTO's objective is to figure out how soon the organization must recover, which in turn determines the kind of measures it must put in place and the amount of money that should be put into ensuring business continuity.
- The Recovery Point Objective (RPO) focuses on the data and the loss tolerance of the organization of the data. RPO is determined by analyzing the time frame between data backups and possibly the amount of data loss.
- The process for communicating with those who are crucial to the organization, such as workers, vendors, and customers, should be included in the communication strategy. The procedure should include when and how to get in touch with the staff, along with backup options in case some regular means of communication become unavailable during an incident.
- A strategy for employee protection and safety in the case of various disasters (such as fire, storm, intruder, etc.) must be incorporated in all disaster recovery plans. Emphasize recovery strategy on getting local employees to safety and think about how distant workers may assist with more time-consuming activities.
- Every item in an organization's digital and physical inventory should be documented in the disaster recovery plan. This will simplify the assessment of insurance claims. Create a list of priorities of equipment and programs for digital inventory.

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

https://t.me/learningnets

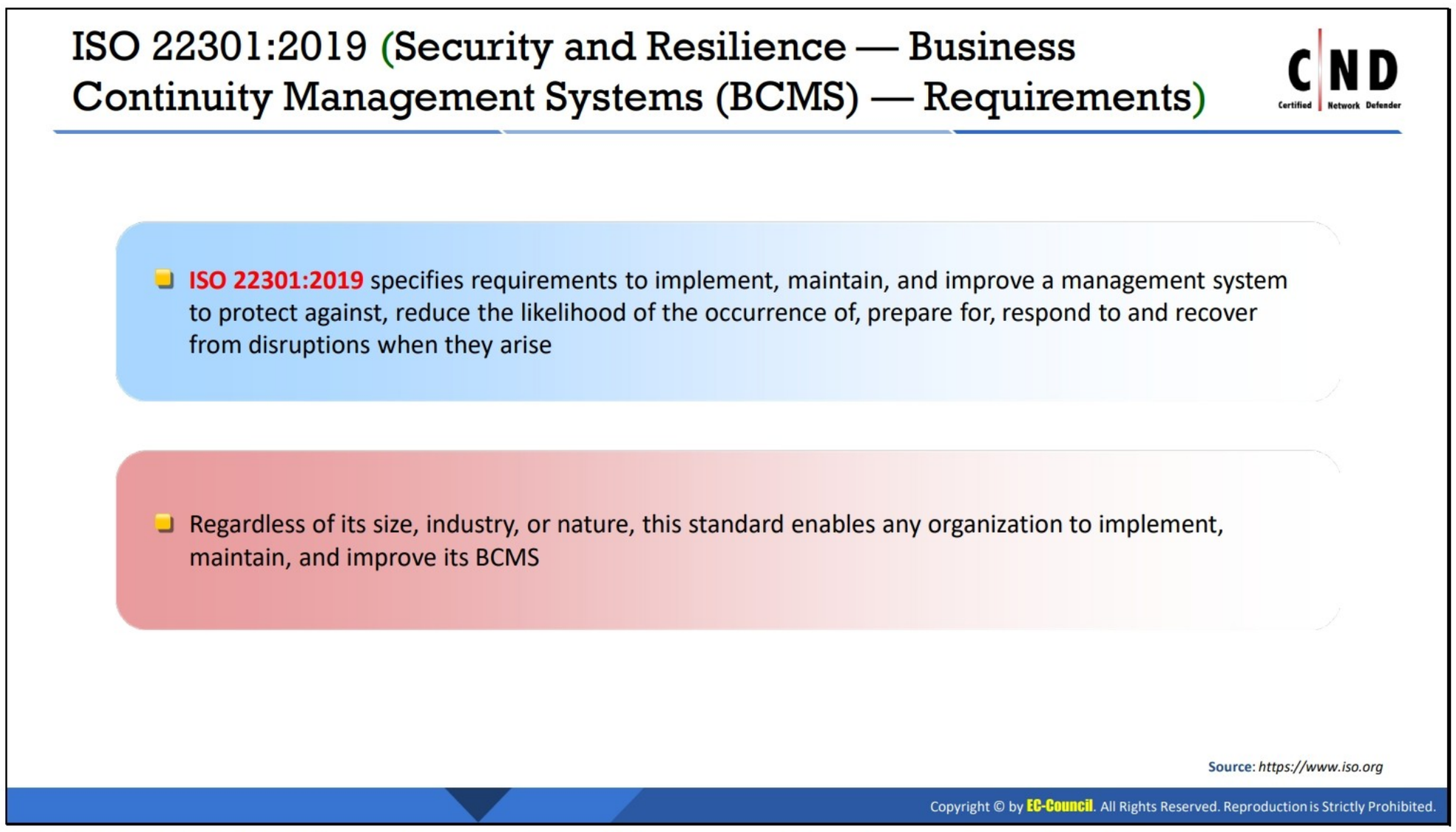


LO#04: Discuss BC/DR Standards

The objective of this section is to discuss the various standards related to BC/DR including the ISO 22301:2019, the ISO 22313:2012, and the ISO/IEC 27031:2011.

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

https://t.me/learningnets



ISO 22301:2019 (Security and Resilience — Business Continuity Management Systems (BCMS) — Requirements)

Source: https://www.iso.org

The ISO 22301:2019 indicates the significance of implementing, maintaining, and improving the system designed to protect an organization from disruptions, equip it to respond to and recover from disruptions when they arise, and reduce the likelihood of their occurrence.

"The requirements specified in the ISO 22301:2019 are generic and intended to be applicable to all organizations, or parts thereof, regardless of the type, size, and nature of the organization. The extent of the application of these requirements depends on the organization's operating environment and complexity."

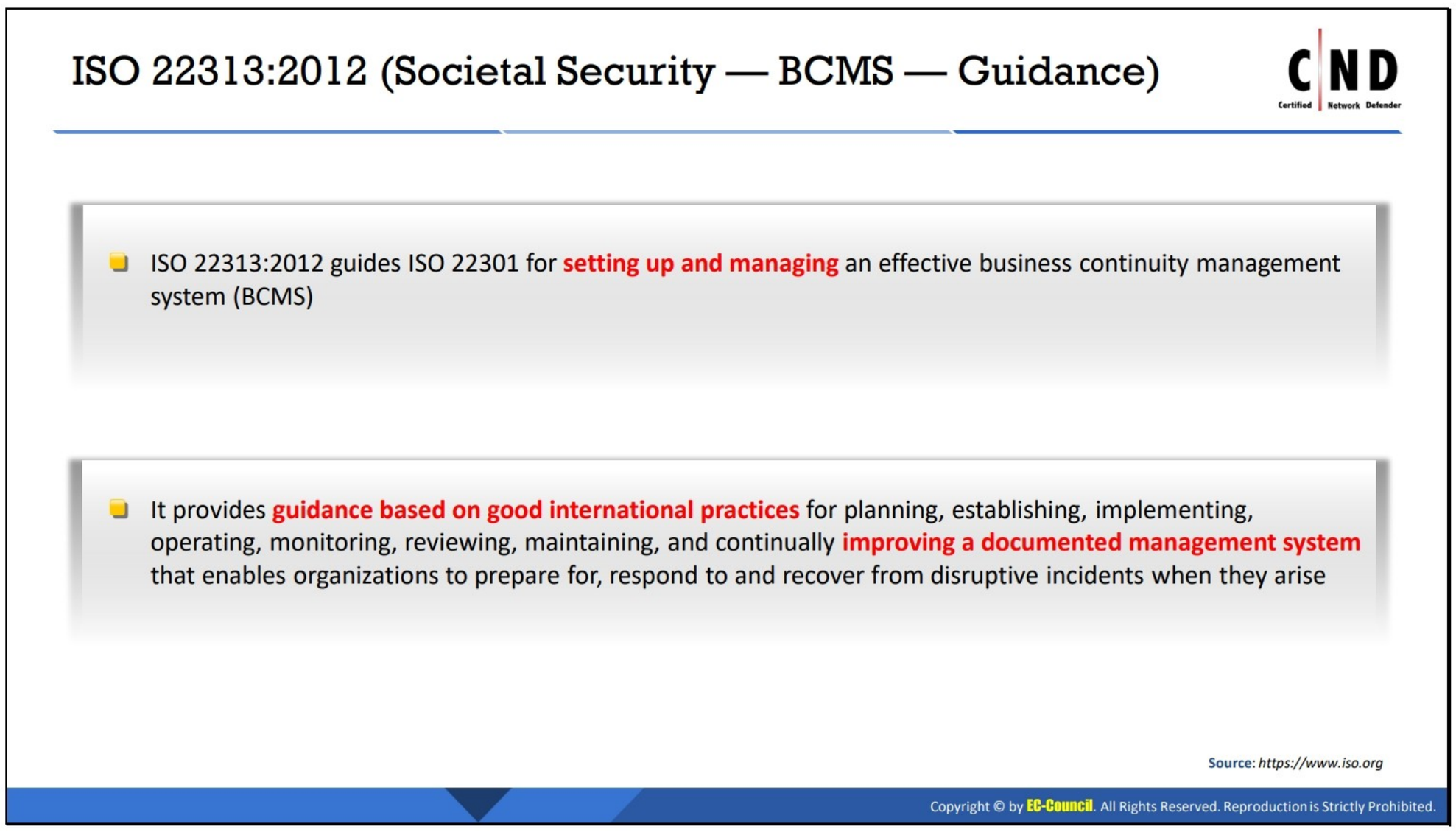
The ISO 22301:2019 is applicable to all types and sizes of organizations that:

- Implement, maintain, and improve business continuity management systems (BCMS);
- Seek to ensure conformity with the stated BC policy;
- Aim to deliver products and services continually at an acceptable predefined capacity during a disruption; and
- Seek to enhance resilience through the effective application of the BCMS.

The ISO 22301:2019 can be used to assess an organization's ability to meet own BC needs and obligations.

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

https://t.me/learningnets



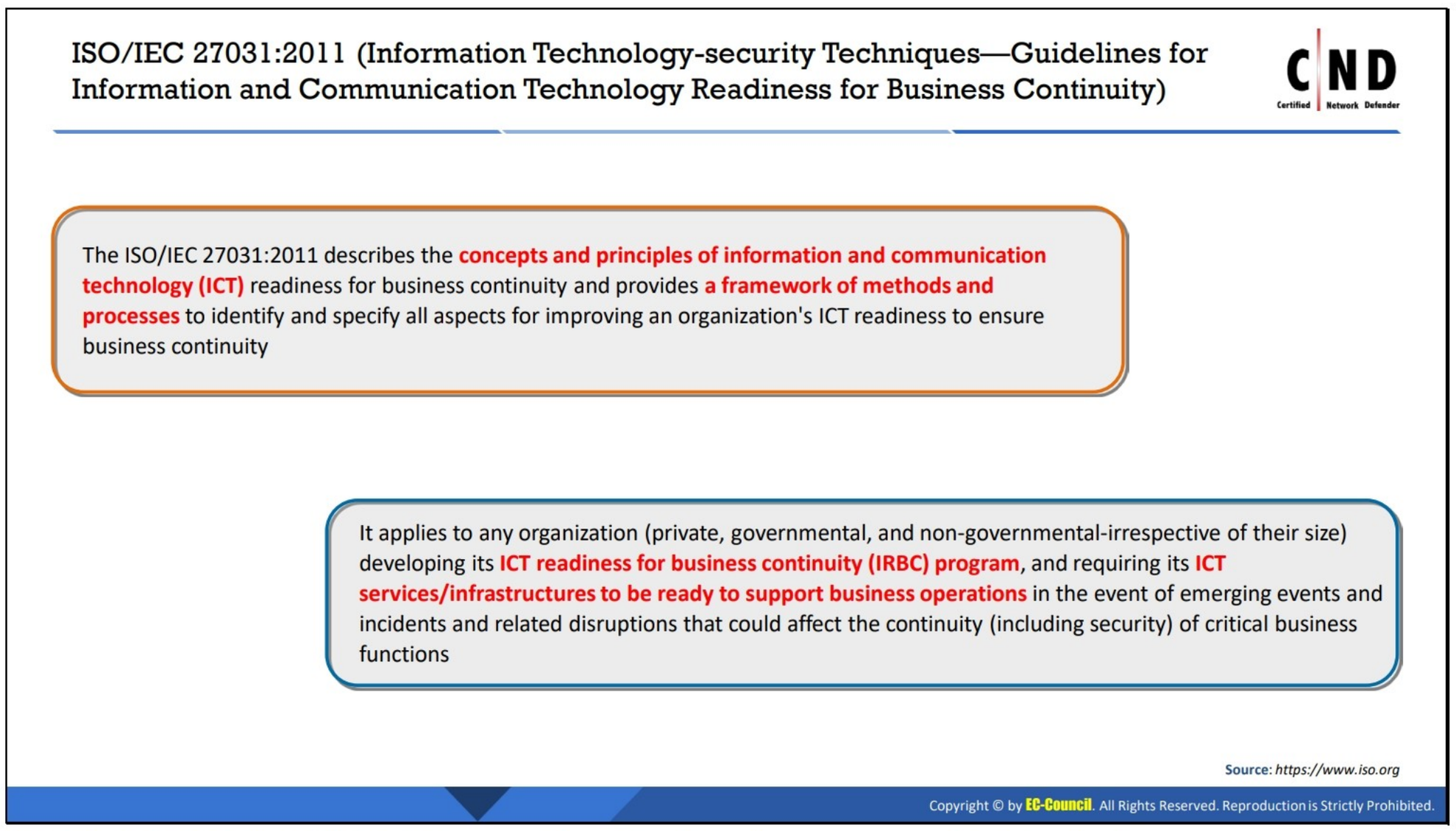
ISO 22313:2012 (Societal Security — BCMS — Guidance)

Source: https://www.iso.org

"The ISO 22313:2012 for BCMS provides guidance based on good international practices for planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving a documented management system that enables organizations to prepare for, respond to, and recover from disruptive incidents when they arise. It is not the intent of ISO 22313:2012 to imply uniformity in the structure of a BCMS; but, it is important for an organization to design a BCMS that is appropriate to its needs and that meets the requirements of its interested parties. These needs are shaped by legal, regulatory, organizational and industry requirements, the products and services, the processes employed, the environment in which it operates, the size and structure of the organization and the requirements of its interested parties."

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

https://t.me/learningnets



ISO/IEC 27031:2011 (Information Technology-security Techniques—Guidelines for Information and Communication Technology Readiness for Business Continuity)

Source: https://www.iso.org

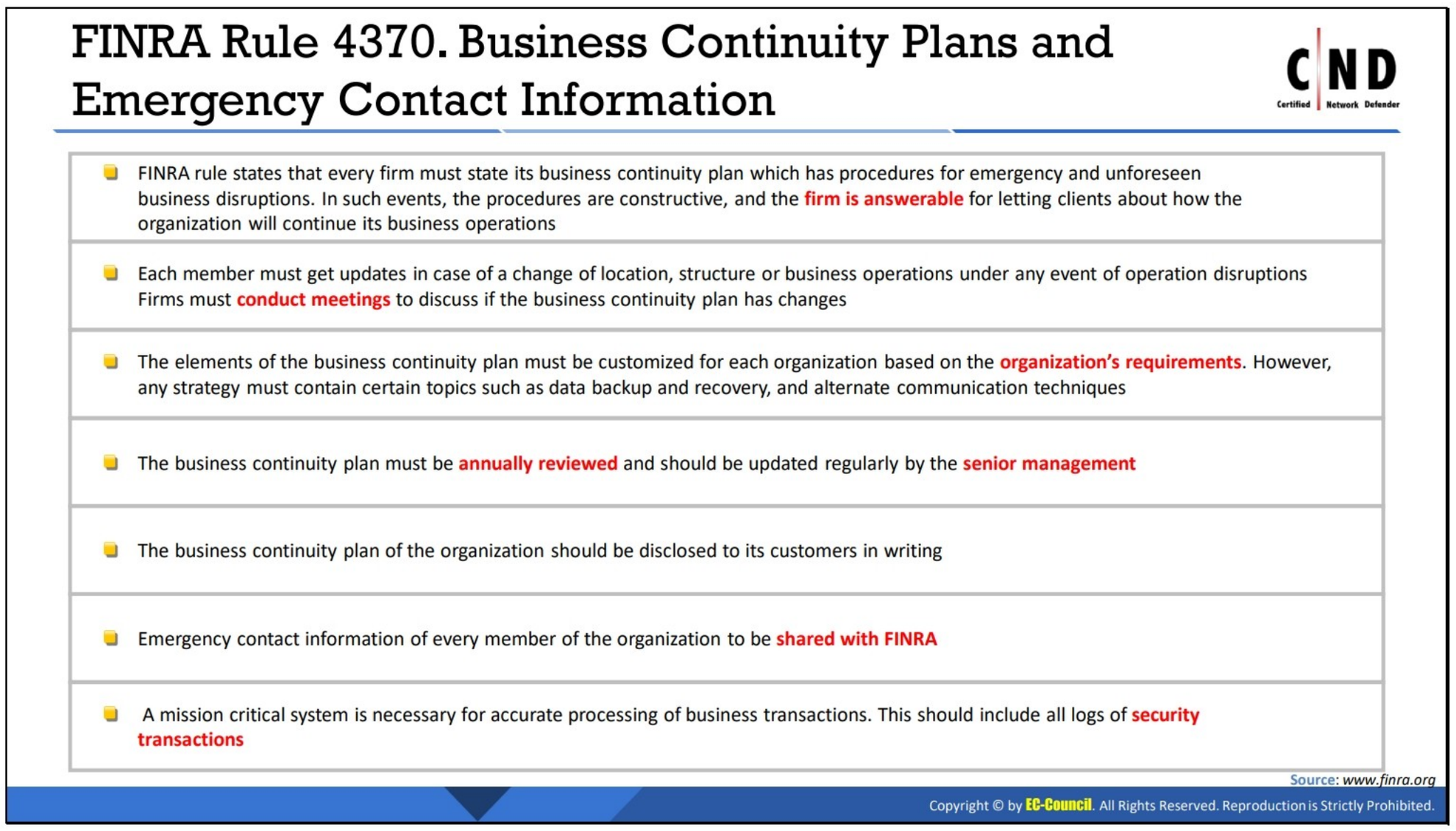
"The ISO/IEC 27031:2011 describes the concepts and principles of information and communication technology (ICT) readiness for business continuity and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. It applies to any organization (private, governmental, and non-governmental—irrespective of their size) developing its ICT readiness for the business continuity (IRBC) program and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents and related disruptions that could affect continuity (including security) of critical business functions. It also enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner."

"The scope of ISO/IEC 27031:2011 encompasses all events and incidents (including security-related) that could have an impact on ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services."

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

https://t.me/learningnets

Technet24



FINRA Rule 4370. Business Continuity Plans and Emergency Contact Information

Financial Industry Regulatory Authority (FINRA) is a government-authorized, not-for-profit organization that establishes rules and regulations to ensure integrity. Some of the key rules of FINRA include the following:

- Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member to meet its existing obligations to customers. In addition, such procedures must address the member's existing relationships with other broker-dealers and counterparties. The business continuity plan must be made available promptly upon request to FINRA staff.
- Each member must update their plan in the event of any material change to the member's operations, structure, business, or location. Each member must also conduct an annual review of its business continuity plan to determine whether any modifications are necessary in light of changes to the member's operations, structure, business, or location.
- The elements that comprise a business continuity plan are flexible and may be tailored to the size and needs of a member. Each plan, however, must at a minimum, address:
    - Data back-up and recovery (hard copy and electronic)
    - All mission-critical systems
    - Financial and operational assessments
    - Alternate communications between customers and the member
    - Alternate communications between the member and its employees

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

https://t.me/learningnets

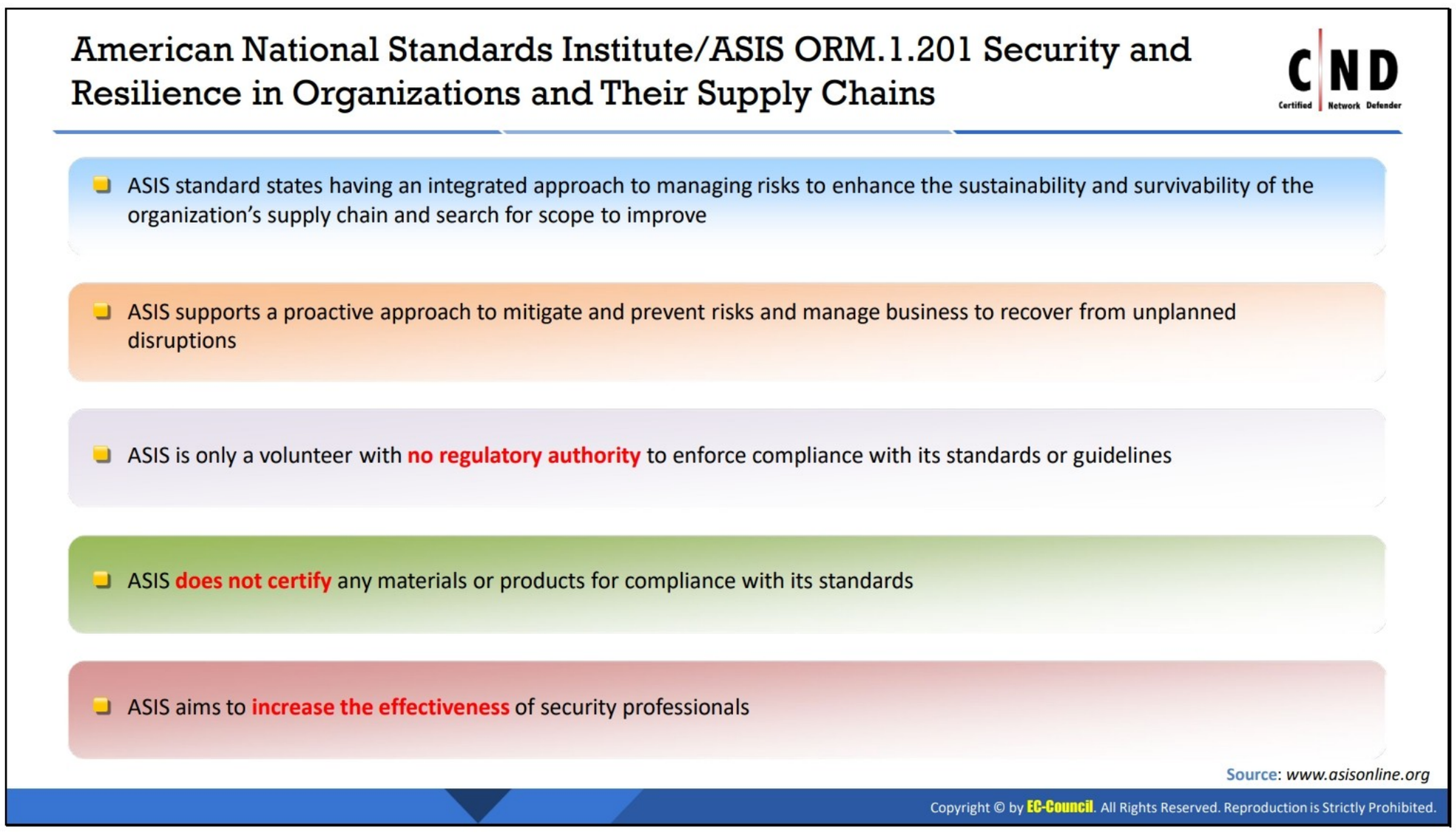
- Alternate physical location of employees
- Critical business constituent, bank, and counter-party impact
- Regulatory reporting
- Communications with regulators

- How the member will assure customers' prompt access to their funds and securities if the member determines that it is unable to continue its business.
- Members must designate a member of senior management to approve the plan and he or she shall be responsible for conducting the required annual review. The member of senior management must also be a registered principal.
- Each member must disclose to its customers how its business continuity plan addresses the possibility of future significant business disruption and how the member plans to respond to events of varying scope. At a minimum, such disclosure must be made in writing to customers at account opening, posted on the member's website (if the member maintains a website), and mailed to customers upon request.
- Each member shall report to FINRA, via such electronic or other means as FINRA may specify prescribed emergency contact information for the member. The emergency contact information for the member includes the designation of two associated persons as emergency contact persons. At least one emergency contact person shall be a member of senior management and a registered principal of the member. If a member designates a second emergency contact person who is not a registered principal, such person shall be a member of senior management who has knowledge of the member's business operations. A member with only one associated person shall designate as a second emergency contact person an individual, either registered with another firm or nonregistered, who has knowledge of the member's business operations (e.g., the member's attorney, accountant, or clearing firm contact).
- Each member must promptly update its emergency contact information, via such electronic or other means as FINRA may specify, in the event of any material change. With respect to the designated emergency contact persons, each member must identify, review, and, if necessary, update such designations in the manner prescribed by Rule 4517.
- "Mission critical system" means any system that is necessary, depending on the nature of a member's business, to ensure prompt and accurate processing of securities transactions, including, but not limited to, order taking, order entry, execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts and the delivery of funds and securities.
- "Financial and operational assessment" means a set of written procedures that allow a member to identify changes in its operational, financial, and credit risk exposures.

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

https://t.me/learningnets

Technet24

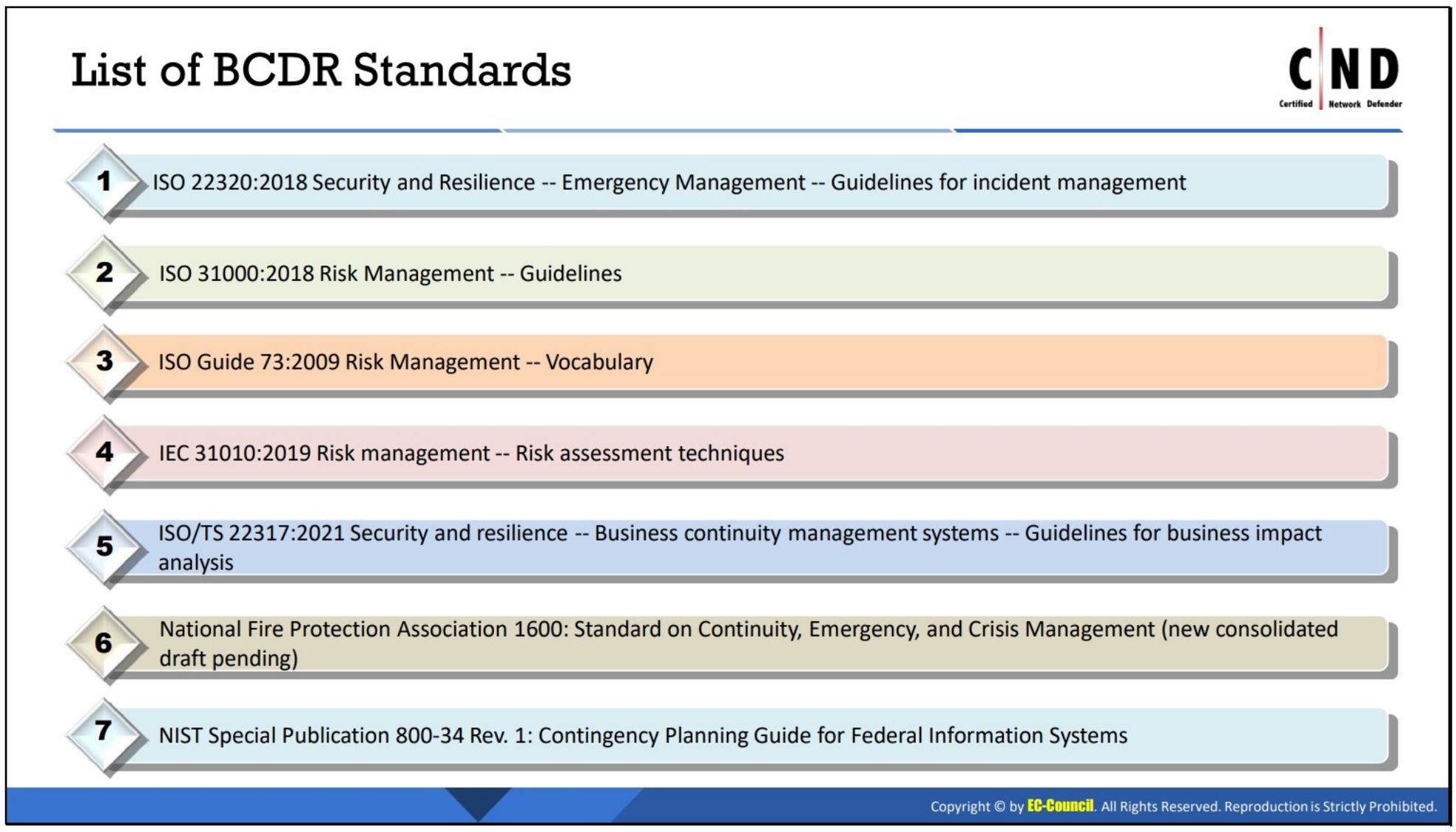


American National Standards Institute/ ASIS ORM.1.201 Security and Resilience in Organizations and Their Supply Chains

- This ASIS standard recognizes the complex risk landscape facing organizations and their supply chains requires an integrated, comprehensive, and systematic risk-based approach for managing risks to enhance sustainability, survivability, and resilience as well as identify and pursue opportunities for improvements.
- The standard emphasizes proactive risk and business management to support a process of prevention, protection, preparedness, readiness, mitigation, response, continuity, and recovery from undesirable and disruptive events.
- ASIS is a volunteer, nonprofit professional society with no regulatory, licensing or enforcement power over its members or anyone else.
- ASIS does not accept or undertake a duty to any third party because it does not have the authority to enforce compliance with its standards or guidelines.
- ASIS does not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards.
- The mission of the ASIS standards and guidelines is within a voluntary, nonproprietary, and consensus-based process, utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS members, security professionals, and the global security industry.

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

https://t.me/learningnets



List of BCDR Standards

Business continuity (BC) and disaster recovery (DR) are two types of approaches that promote a company's ability to continue operations after an undesirable incident.

BCDR techniques help an organization recover quickly from issues, lower the risk of data loss and damage to its reputation, and enhance operations while reducing the possibility of emergencies.

The following are the sampling of standards:

- **ISO 22320:2018 Security and resilience -- Emergency management -- Guidelines for incident management**

  The incident response requirements are described in this business continuity standard, along with an essential emphasis on command and control, operational data, and communication with incident response organizations.

- **ISO 31000:2018 Risk Management --Guidelines**

  The nature, kindness, and complexity of an organization's activities have no impact on how this generic risk management approach should be used. The key areas are risk management and effective resource allocation.

- **ISO Guide 73:2009 Risk Management – Vocabulary**

  This standard aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.

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

https://t.me/learningnets

Technet24

- **IEC 31010:2019 Risk management -- Risk assessment techniques**

  This standard provides guidance on the selection and application of techniques for assessing risk in a wide range of situations. The techniques are used to assist in making decisions where there is uncertainty, to provide information about risks, and as part of a process for managing risk.

- **ISO/TS 22317:2021 Security and resilience -- Business continuity management systems -- Guidelines for business impact analysis**

  This standard provides guidelines for an organization to implement and maintain a formal and documented Business Impact Analysis (BIA) process appropriate to its needs. It does not prescribe a uniform process for performing a Business Impact Analysis.

- **National Fire Protection Association 1600: Standard on Continuity, Emergency, and Crisis Management (new consolidated draft pending)**

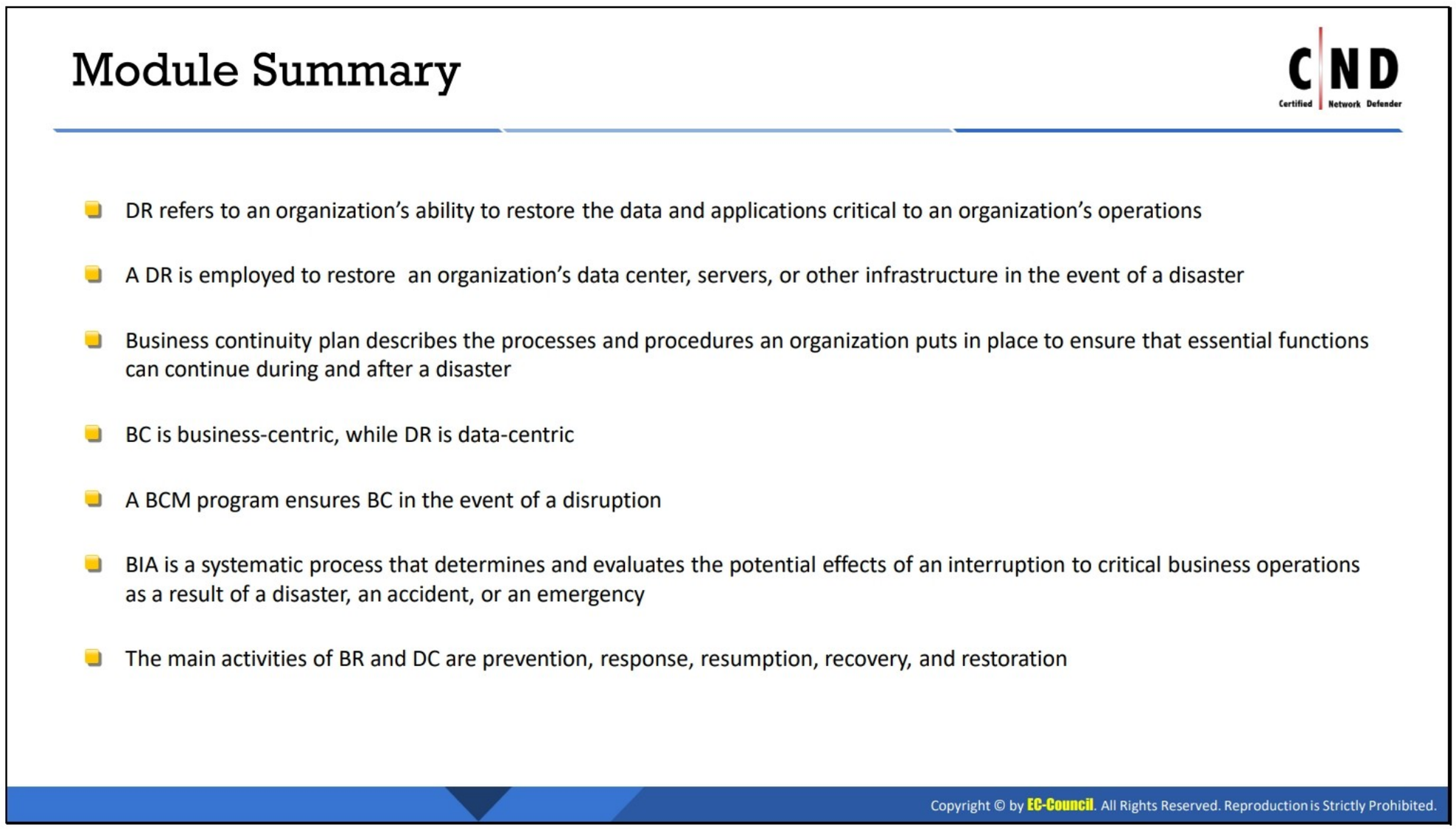
  This standard establishes a common set of criteria for emergency management and business continuity programs; mass evacuation, sheltering, and re-entry programs; and the development of pre-incident plans for personnel responding to emergencies.

- **NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems**

  This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle. It also provides guidance to help personnel evaluate information systems and operations to determine contingency planning requirements and priorities.

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

https://t.me/learningnets



Module Summary

The following key points have been discussed in this module:

- DR refers to an organization's ability to restore the data and applications critical to an organization's operations. A DR is employed to restore an organization's data center, servers, or other infrastructure in the event of a disaster.
- An organization's BCP specifies the processes and procedures that must be implemented to ensure BC.
- BC is business-centric, while recovery is data-centric.
- The main activities of a DR and BC are prevention, response, resumption, recovery, and restoration.

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

https://t.me/learningnets

Technet24