

Introduction to Security Operations

Lecture 9

HCIA-Security

Prepared by
Dr. Abdelrhman Ahmed

- **In the current information age, security is the foremost concern of global enterprises. The threat of cyber attacks and data breach means security operations are a necessity to ensure the safe and continuous use of enterprise services. These slides describe the basic concepts and prerequisites of security operations.**

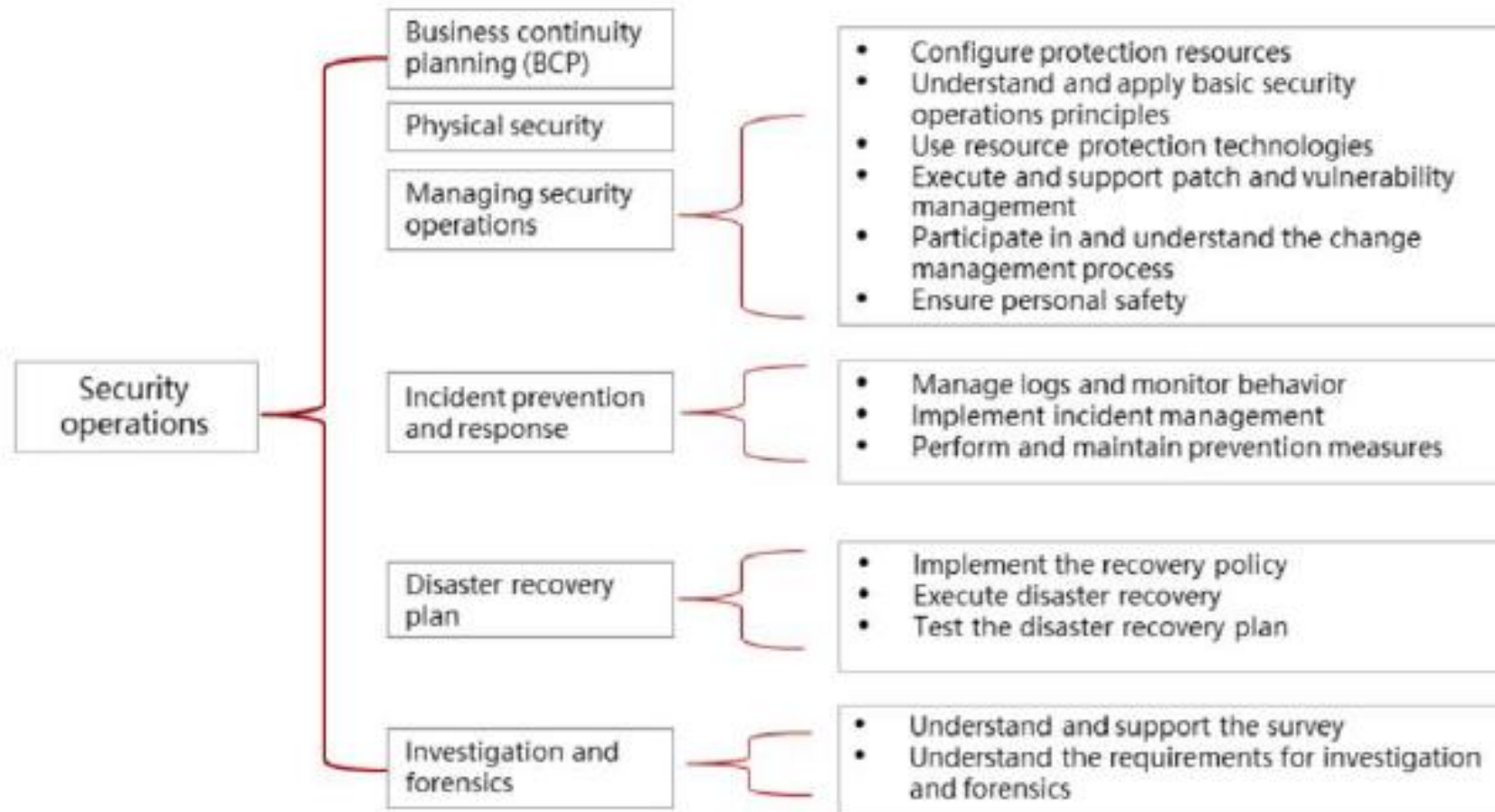
Objectives

- **Upon completion of this course, you will be able to:**
 - ❑ **Learn the concepts related to security operations**
 - ❑ **Learn the content of security operations**

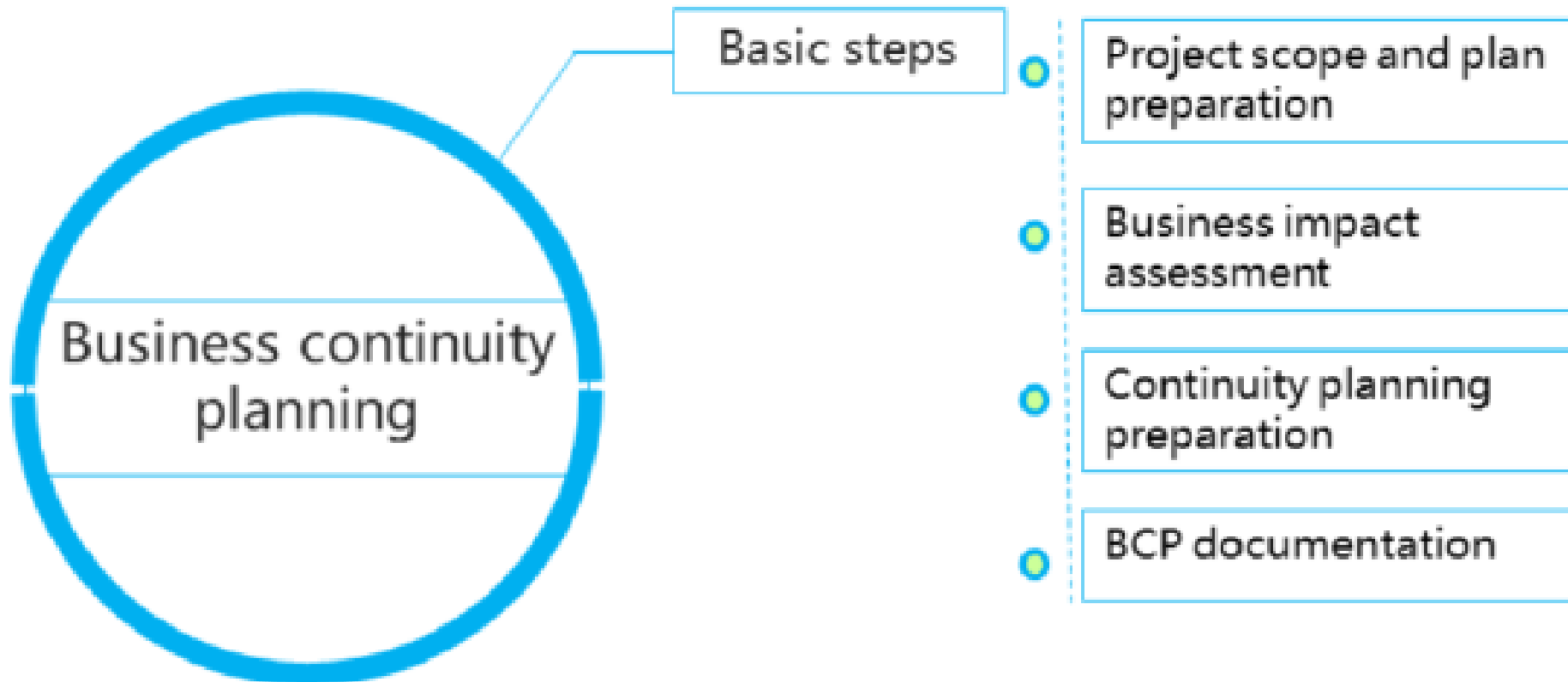
Concept of Security Operations

- In the initial stage of enterprise information security construction, the enterprise's priority is to purchase a series of security devices and deploy them at each protocol layer to ensure the stable running of services.
- As security issues frequently occur, effective security operations cannot be achieved solely through security devices. Successful security operations are the combination of resources, processes, and management, to ensure the secure and stable running of enterprise services.

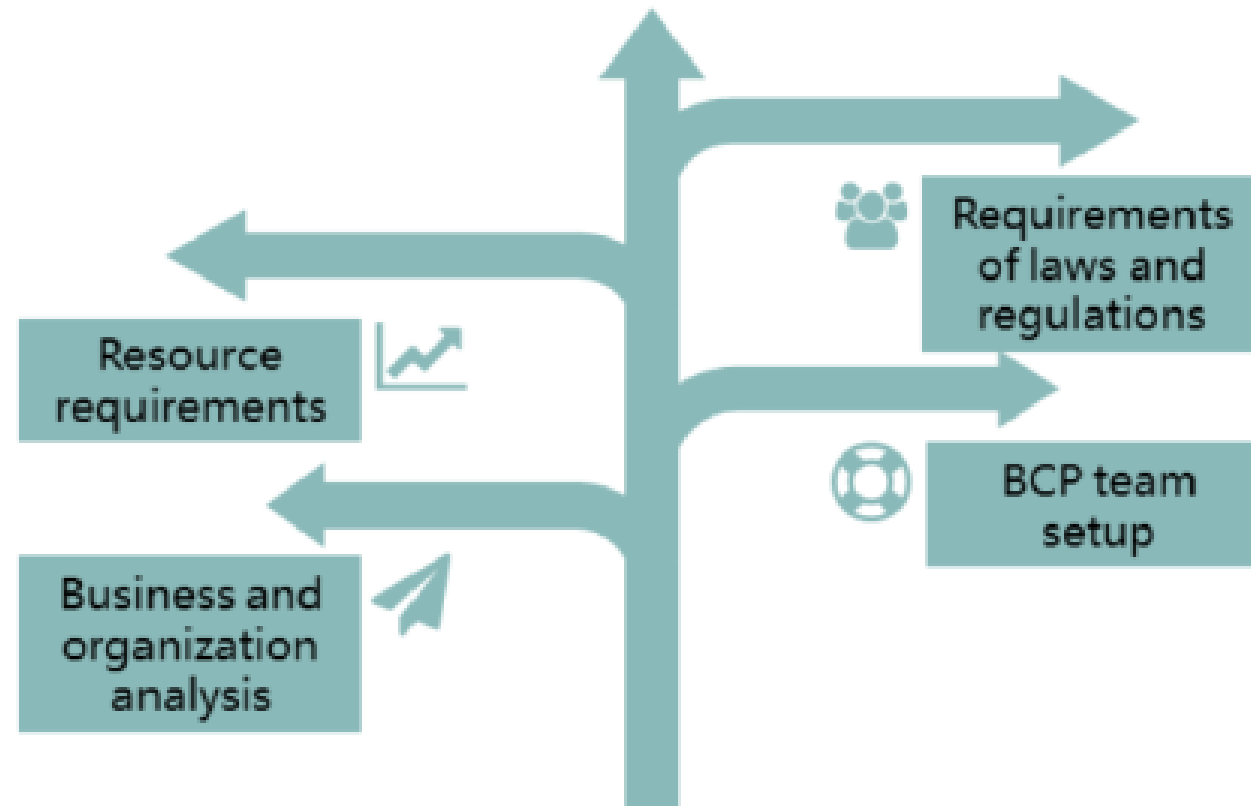
- Security operations involve various requirements. The following lists the basic operations conditions for security operations.



Business Continuity Planning



- Any process or plan must be formulated based on the actual business scale and nature of the organization, complying with the corporate culture and relevant laws. The following lists the specific requirements for the non-rated project scope at the initial stage of the plan.

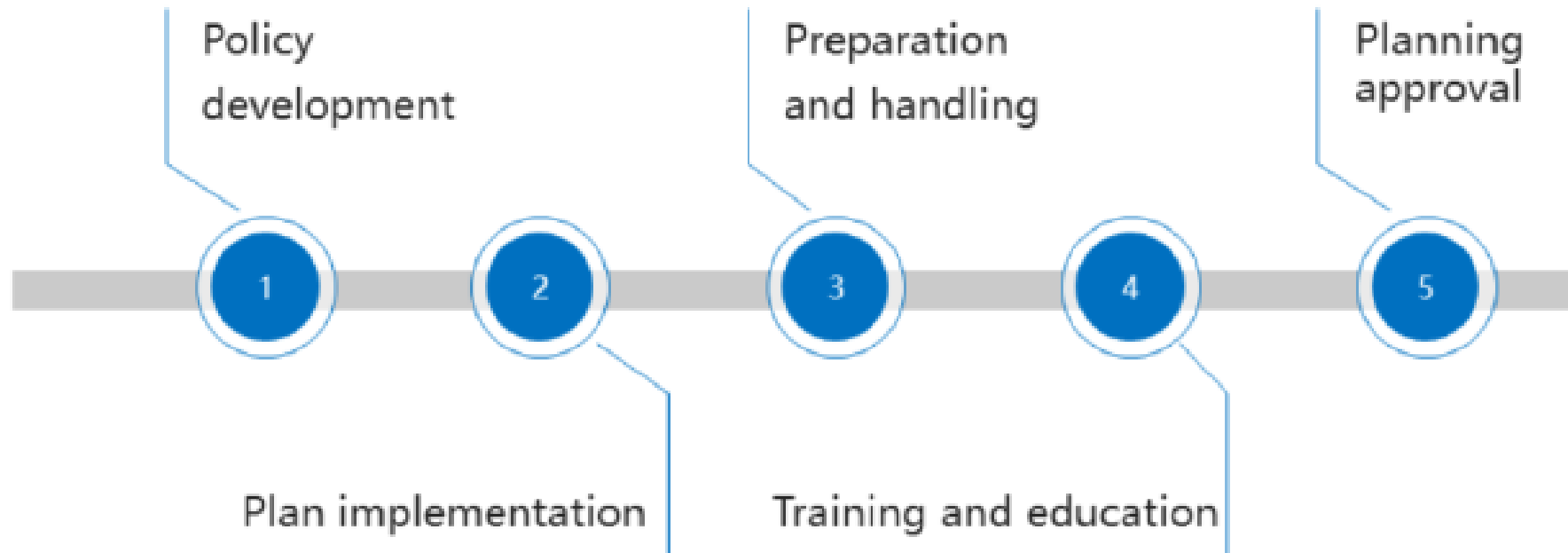


Business Impact Assessment

- **Business Impact Assessment identifies which resources can sustain the development of the organization. It also evaluates threats to resources, the likelihood of each threat, and their potential impact on businesses. Business Impact Assessment consists of:**



- Two phases are mainly used to determine the BCP working process and protect the limited sequence of business assets. In the continuity planning preparation phase, focus is on the development and implementation of the continuity policy, and the following tasks are involved:



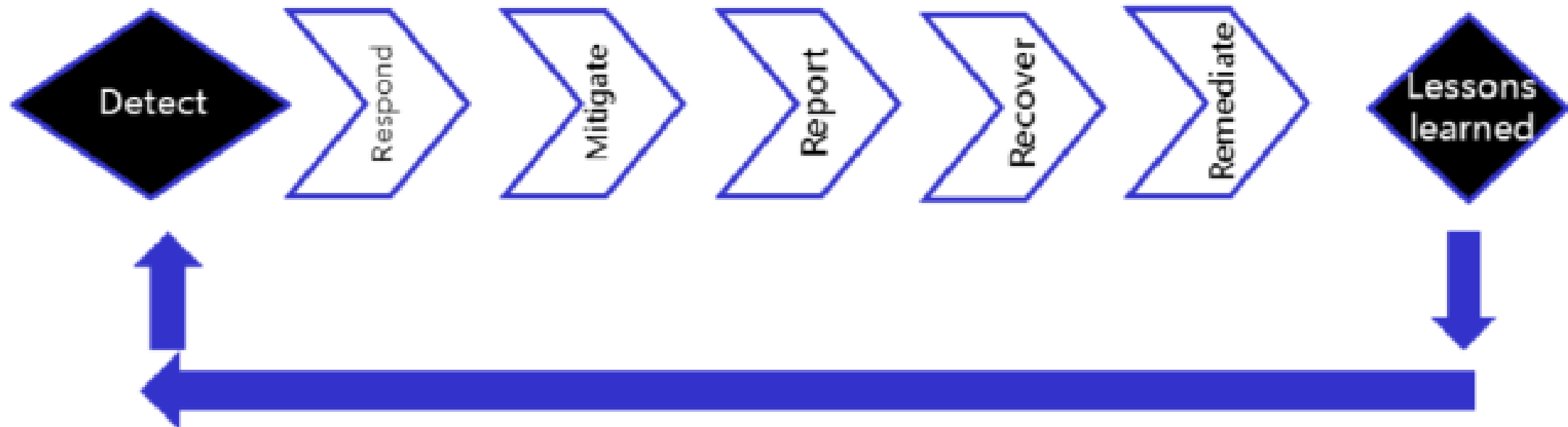
BCP Documentation

- **BCP documentation provides BCP personnel with guidance in the event of an emergency. In addition, the document records the modification history and provides reference for subsequent handling of similar incidents or document modification. The document must contain the following information:**

- ☐ **Objectives of the continuity planning**
- ☐ **Importance statement**
- ☐ **Statement of organization responsibilities**
- ☐ **Declaration of urgency and time limit**
- ☐ **Risk assessment**
- ☐ **Acceptable risk/Risk mediation**
- ☐ **Major record plan**
- ☐ **Guidelines for responding to emergencies**
- ☐ **Maintenance**
- ☐ **Tests and exercises**

Incident Response Management

- Not all threats can be prevented, but BCP provides process guidance for handling emergencies and responding to threat incidents as soon as possible to minimize the impacts on organizations.



Disaster Recovery Plan

- When a service is interrupted due to a disaster, the disaster recovery plan takes effect, instructing the emergency response personnel to restore services to the normal state.
- The disaster recovery plan includes the following steps:

**Execute the
disaster
recovery plan**



**Implement the
recovery policy**



**Test the disaster
recovery plan**

Investigation

- Before taking measures, it needs to be determined whether an attack has occurred. After an attack occurs, enterprises must investigate the incident and collect evidence. The investigation aims to find out what happened and the extent of the damage.



Evidence

- In order to successfully prosecute a crime, sufficient evidence must be provided to prove the crime. Evidence types include:
 - ☐ Physical evidence
 - ☐ Documentary evidence
 - ☐ Verbal evidence
- Evidence must be acceptable:
 - ☐ Evidence must be related to the determination of facts.
 - ☐ Evidence must be related to the event
 - ☐ Evidence must be legally obtained.
- Evidence type:
 - ☐ Physical evidence: objective evidence, such as objects
 - ☐ Documentary evidence: written content, such as computer logs
 - ☐ Verbal evidence: witnesses' testimony

Investigation and Forensics Process





Thank You