IRP

Incident Terminology:

1. **Breach**: Loss of control, authorized disclosure, unauthorized acquisition, compromised
2. **Event**: An observable occurrence in the information system.
3. **Exploit**: A particular attack which happened because of system vulnerability.
4. **Incident**: An event that actually or potentially jeopardized the confidentiality, integrity and availability of information systems.
5. **Threat**: Any circumstance or event with potential to adversely impact on organizational assets.

Component of Incident Response Plan: (*An Incident Response Plan outlines the **procedures** and protocols that an organization follows when a cybersecurity incident occurs.*)

1. **Preparation:**
    a. Develop policy
    b. Incident response team
    c. Practices Risk identification
    d. Identify Roles and responsibilities
2. **Detection & analysis:**
    a. Monitor all possible attack
    b. Prioritize Incident Response
    c. Standralize incident documentation
3. **Containment & eradication:**
    a. Gather evidence
    b. Choose containment strategy
    c. Identify Attacker
    d. Isolate the Attack
4. **Post-Incident Activity:**
    a. Identify the documents that may need to be retained
    b. Document lesson learned

BCP

Business Continuity Plan: *(A Business Continuity Plan outlines the procedures and strategies that an organization employs to ensure that essential business functions can continue or be rapidly restored following a disruptive event.)*

Planning -> **Preparation** -> **Response** -> **Recovery**

The goal of a BCP is to maintain business continuity by:

- Identifying **critical business processes and resources**
- **Assessing** risks and vulnerabilities
- **Implementing preventive** measures
- Developing **response and recovery strategies**
- **Establishing communication** and coordination mechanisms.

A major incident will interrupt business for an unacceptable length of time, and the organization cannot just follow an incident plan but must move toward business continuity.

It focuses on the critical products & services that the organization provides & ensures those important areas can continue to operate even at a reduced level of performance until business returns to normal.

Key components of a BCP include

- business impact analysis
- risk assessment and mitigation strategies
- alternate work arrangements
- data backup
- recovery plans
- crisis communication plans
- testing and exercising procedures to ensure readiness.

Components of Business Continuity Plan:

1. List of BCP members
2. Immediate response procedure checklist
3. Notification system for all members of the BCP team
4. How/when enact the plan

DRP

DRP: (Disaster Recovery refers to the process of restoring IT systems, infrastructure, and data following a disruptive event that affects the organization's ability to operate normally.)

The goal of Disaster Recovery is to:

- Recover IT resources
- Resume critical business functions as quickly as possible to minimize downtime, financial losses, and reputational damage.

Key components of a DR plan include:

- Data backup and recovery strategies
- System redundancy and failover mechanisms
- Disaster recovery infrastructure and facilities
- Data replication and synchronization, and testing and validation procedures to ensure the **effectiveness of recovery processes.**
- Checklist for critical disaster recovery team

Connection between : IRP <-> BCP <-> DRP

Incident Response Plans focus on addressing security incidents and breaches, ***Business Continuity Plans*** focus on maintaining essential business functions during disruptive events, and ***Disaster Recovery plans*** focus on restoring IT systems and data following a disaster or disruption.

Prevention and Preparedness:

- Incident Response Plans focus on the **immediate response to security incidents**, but they often include preventive measures and preparedness activities to minimize the likelihood and impact of incidents. This can involve implementing security controls, conducting security awareness training, and performing risk assessments.
- Business Continuity Plans **encompass broader risk management strategies**, including preventive measures to mitigate the impact of potential disruptions. These measures can include redundancy in critical systems, backup power supplies, and geographic diversification of operations to reduce the likelihood of widespread disruptions.
- Disaster Recovery Plans primarily **focus on preparing for and responding to catastrophic events** that could affect IT systems and data. This involves implementing backup and recovery procedures, establishing redundant data centers, and ensuring the availability of resources necessary for recovery efforts.

Response and Recovery:

- Incident Response Plans guide the **immediate response to security incidents, including the containment of threats, the investigation of breaches, and the restoration of normal operations**. They often involve coordination between IT security teams, incident response teams, legal departments, and other stakeholders.
- Business Continuity Plans provide a **framework for responding to broader disruptions that impact business operations**, such as natural disasters, supply chain disruptions, or public health emergencies. They include procedures for relocating staff, activating backup facilities, and maintaining communication with stakeholders during crises.

- Disaster Recovery Plans **focus specifically on restoring IT systems** and data following a disruptive event. They outline procedures for recovering data from backups, rebuilding infrastructure, and resuming critical IT services to support business operations.

Testing and Improvement:

- Incident Response Plans are **often tested through simulated security incidents, tabletop exercises, and red team/blue team exercises** to evaluate the organization's ability to detect, respond to, and recover from cyber threats.
- Business Continuity Plans are **tested through exercises such as business impact analysis, tabletop exercises, and full-scale** simulations to assess the organization's ability to maintain essential functions and services during disruptions.
- Disaster Recovery Plans are **tested through disaster recovery drills, failover tests, and data recovery exercises** to validate the effectiveness of backup and recovery procedures and ensure rapid restoration of IT systems and data.