Unit VII: Continuity Planning

- Incidence Response Planning
- Business continuity planning
- Disaster recovery planning

Incident Response Planning (IRP)

- **Definition**: A structured approach to detect, respond to, and recover from security incidents such as cyberattacks, data breaches, or system failures.
- **Objectives**:
  - Minimize damage and reduce recovery time.
  - Contain threats quickly to prevent escalation.
  - Preserve evidence for forensic analysis.
- **Key Components**:
  - **Preparation**: Define roles, responsibilities, and communication channels.
  - **Detection & Analysis**: Monitor systems for anomalies, identify incidents, and assess severity.
  - **Containment**: Short-term (stop immediate damage) and long-term (prevent recurrence).
  - **Eradication**: Remove malicious code, close vulnerabilities.
  - **Recovery**: Restore systems to normal operation.
  - **Lessons Learned**: Document findings, update policies, and improve defenses.
- **Example**: Responding to a ransomware attack by isolating infected systems, restoring backups, and notifying stakeholders.

2. Business Continuity Planning (BCP)

- **Definition**: A proactive plan ensuring that essential business functions continue during and after a disruption.
- **Objectives**:
  - Maintain critical operations during crises.
  - Protect employees, assets, and reputation.
  - Reduce financial and operational impact.
- **Key Components**:
  - **Risk Assessment**: Identify threats (natural disasters, cyberattacks, pandemics).
  - **Business Impact Analysis (BIA)**: Determine which processes are critical and the impact of downtime.
  - **Strategies**: Alternate work sites, remote work, supply chain diversification.
  - **Plan Development**: Document procedures for continuity of operations.
  - **Testing & Training**: Regular drills to ensure staff readiness.
- **Example**: During a pandemic, enabling remote work infrastructure to keep operations running.

3. Disaster Recovery Planning (DRP)

- **Definition**: A subset of BCP focused specifically on restoring IT systems, applications, and data after a disaster.
- **Objectives**:
  - Rapid recovery of technology infrastructure.
  - Minimize downtime and data loss.
  - Ensure compliance with legal and regulatory requirements.
- **Key Components**:
  - **Recovery Point Objective (RPO)**: Maximum acceptable data loss (e.g., 4 hours of data).
  - **Recovery Time Objective (RTO)**: Maximum acceptable downtime (e.g., 12 hours).
  - **Backup Strategy**: On-site, off-site, or cloud-based backups.
  - **Disaster Scenarios**: Natural disasters, cyberattacks, hardware failures.
  - **Testing**: Simulated recovery exercises to validate effectiveness.
- **Example**: Restoring critical databases from cloud backups after a server room flood.

🔑 Comparison Table

Aspect	Incident Response (IRP)	Business Continuity (BCP)	Disaster Recovery (DRP)
Focus	Security incidents	Overall business functions	IT systems & data
Goal	Contain & resolve threat	Maintain operations	Restore technology
Scope	Cybersecurity & events	Organization-wide	IT infrastructure
Timeframe	Immediate response	During & after disruption	Post-disaster recovery
Example	Ransomware containment	Remote work during crisis	Database restoration

⚠ Risks & Challenges

- **IRP**: Failure to detect incidents early can lead to severe breaches.
- **BCP**: Lack of testing makes plans ineffective during real crises.

- **DRP**: Inadequate backups or slow recovery can cripple operations.