Disaster Recovery Training: 2 days

Day 1: Foundations and Planning

1. Introduction to Disaster Recovery (DR)

- Understanding the scope and significance of DR
- Differentiating between Disaster Recovery, Business Continuity, and Crisis Management
- Regulatory and compliance requirements

2. Types of Disasters and Risk Assessment

- Natural, technical, and human-caused disasters
- Risk identification and impact analysis
- Threat modeling and vulnerability assessment

3. Business Impact Analysis (BIA)

- Defining Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Identifying critical business functions and assets
- Mapping dependencies and interrelations

4. Disaster Recovery Planning (DRP)

- Steps in creating a disaster recovery plan
- Roles and responsibilities in DR
- Selecting recovery strategies (e.g., cold site, hot site, cloud-based DR)

5. Data Backup and Recovery Techniques

- Backup types (full, incremental, differential)
- Data storage options (on-premise, cloud, hybrid)
- Recovery testing and verification methods

6. Case Study and Group Discussion

- Analyze real-world disaster recovery scenarios
- Group activity to draft a sample DR plan

Day 2: Implementation and Execution

1. Disaster Recovery Technologies
    - Virtualization and disaster recovery
    - Cloud-based DR solutions (e.g., Azure Site Recovery, AWS Disaster Recovery)
    - Automated DR tools and platforms
2. Incident Response and Crisis Communication
    - Coordination with emergency services and stakeholders
    - Communication protocols before, during, and after a disaster
    - Internal and external messaging best practices
3. Testing and Maintenance of DR Plans
    - Types of DR testing (tabletop, simulation, full interruption)
    - Frequency and documentation of tests
    - Plan review, audits, and continuous improvement
4. Legal, Regulatory, and Ethical Considerations
    - DR compliance standards (ISO 22301, NIST, GDPR)
    - Ensuring data security and privacy
    - Ethical decision-making in disaster scenarios
5. Disaster Recovery in IT and Cybersecurity Contexts
    - Cyberattacks and ransomware recovery strategies
    - IT asset restoration and business continuity alignment
    - Recovery of critical infrastructure and applications