EDRP v3 Course Outline

Module 01: Introduction to Disaster Recovery and Business Continuity

- An Introduction to Business Continuity
- An Introduction to Disaster Recovery
- Basic Terminologies of Disaster Recovery & Business Continuity
  - Business Continuity Plan (BCP)
  - Business Impact Analysis (BIA)
  - Disaster Recovery Plan (DRP)
  - Business Continuity Management (BCM)
  - Risk Assessment
  - Recovery Point Objective (RPO)
  - Recovery Time Objective (RTO)
  - Application Recovery
- Disaster Recovery Vs. Business Continuity
- Purpose of Disaster Recovery and Business Continuity
  - Prevention
  - Response
  - Resumption
  - Recovery
  - Restoration
- Trends in Disaster Recovery and Business Continuity
  - Virtualization
  - Offsite Backups
  - Social Media Communications
  - Managed Disaster Recovery
  - Electronic Vaulting
- Best Practices in Disaster Recovery and Business Continuity

Module 02: Business Continuity Management (BCM)

- What is Business Continuity
- What is BCM?
  - Core elements of BCM
- Ownership of BCM
- Scope of BCM
- Benefits of BCM
- Business Continuity Management Framework

  - Understanding the Business and Identifying the Key Processes
  - Devising a BCM Strategy
  - Developing and Implementing the BCM Response
  - Testing, Training, and Maintaining
- Best Practices of BCM
- Business Continuity Standards
  - Plan-Do-Check-Act (PDCA) Model
  - ISO 22301:2012 (Societal Security—Business Continuity Management Systems)
  - ISO 22313:2012 (Societal Security—Business Continuity Management Systems-Guidance)
  - ISO/IEC 27031:2011 (Information Technology-Security Techniques—Guidelines for Information and Communication Technology Readiness for Business Continuity)
  - NFPA 1600 (Standard on Disaster/Emergency Management and Business Continuity Programs)

Module 03: Risk Assessment

- Terminologies Related to Risk in BCP
- What is a Risk?
- Risk Models
  - Terminologies Related to Risk in BCP
  - Threat
  - Vulnerabilities
  - Hazards/Predisposing Conditions
  - Likelihood
  - Impact
- Risk Assessment
- Goals of Risk Assessment
- Assessment Approaches
  - Quantitative Assessment
  - Semi-Qualitative Assessment
  - Qualitative Assessment
- Communicating and Sharing Risk Assessment Information and Results
- Maintaining the Risk Assessment
- Steps in Risk Assessment Process
  - System Characterization

  - Threat Identification
  - Vulnerability Identification
  - Control Analysis
  - Likelihood Determination
  - Impact Analysis
  - Risk Determination
  - Control Recommendations
  - Results Documentation
- Risk Assessment Report
- Best Practices in Risk Assessment
- Risk Management Standards
  - ISO/IEC 27005:2011- Information Security Risk Management
  - ISO 31000:2009- Risk Management (Principles and Guidelines)
  - IEC 31010:2009- Risk Management (Risk Assessment Techniques)
- Case Study

Module 04: Business Impact Analysis (BIA)

- What is Cost Benefit Analysis (CBA)?
  - Recovery Strategies vs. CBA
- What is Business Impact Analysis (BIA)?
- Scope and Objectives of Business Impact Analysis (BIA)
- BIA Terminology
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
  - Maximum Tolerable Period of Disruption (MTPOD)
- Components of BIA
  - Executive Sponsorship
  - Formation of a BCP Committee
  - Identifying the Impact of Critical Business Activities
  - BIA Tools
  - Feedback
  - BIA Process
- Performing BIA
  - Gathering Information
  - Performing a Business Vulnerability Assessment
  - Analyzing the Information
  - Documenting the Results

- ISO/TS 22317:2015 (Societal Security—Business Continuity Management Systems-Guidelines for BIA)
- Case Study

Module 05: Business Continuity Planning (BCP)

- Business Continuity Planning
- Characteristics of Business Continuity Plan
  - Transparent and Certainty
  - Simplified but Robust
  - Availability
  - Prioritized Data
  - Estimated Time and Duration
  - Multiple Backups
  - Appropriately Staffed
  - Comprehensive
  - Use of Advanced Technology and Tools
  - Review, Update and Test
- Key Elements of Business Continuity Policy
  - Introduction / Objective
  - Scope
  - Strategy
  - Statement
  - Roles and Responsibilities
  - Policy Compliance
  - Appendices
- Key Elements of Business Continuity Plan as Part of its Policy
  - Corporate Culture
  - Operations and Team
  - Communication
  - Safety
  - Uninterrupted Access to Resources
  - Testing
- Business Continuity Strategy Design
- Case Study for Business Continuity Strategy Design

Module 06: Data Backup Strategies

- Backup
- Need for Backup
- Types of Backup
  - Full Backup
  - Incremental Backup
  - Differential Backup
  - Synthetic Back
  - Incremental Forever Backup
- 3-2-1 Backup Strategy
- Hot Backup
- Cold Backup
- Types of Backup/ Recovery Sites
  - Cold Site
  - Warm Site
  - Hot Site
  - Colocation Facilities
- Bare Metal Recovery
- Disk Backups
  - Virtual Tape Library (VTL)
  - Disk-to-Disk (D2D)
  - Snapshot
  - Continuous Data Protection (CDP)
- Deduplication
- Cloud Data Recovery
- Cloud Disaster Recovery Blueprint
  - Managed Applications and Managed DR
  - Cloud-based Backup and Restore
  - Replication in the Cloud
- Best Practices in Backup

Module 07: Data Recovery Strategies

- Introduction to Data Recovery
- Recovery Management
- Recovery Management Model Layers
  - Common Management Layer
  - Testing Simulation Layer

    - Analytics and Reporting Layer
    - RPO and RTO Services Layer
    - Protection Technologies Layer
- Types of Data Recovery
    - Logical Data Recovery
    - Physical Data Recovery
- Steps in Data Recovery
    - Evaluation of Storage Media
    - Documentation
    - Actual Recovery
    - Precautions
- Disk-to-Disk-to-Disaster Recovery (3DR)
- Infrastructure Technologies
    - Server Clustering
    - Database Replication
    - High-Availability
    - Failover
    - Point-In-Time Recovery
    - Load Balancing
    - Data Archiving
- Data Protection Continuum
- Data Loss
- Best Practices in Data Recovery

Module 08: Virtualization-Based Disaster Recovery

- What is Virtualization?
- Virtualization and Disaster Recovery
    - Network Virtualization
    - Server Virtualization
    - Operating System (OS) Virtualization
    - Desktop Virtualization
    - Storage Virtualization
    - Data Virtualization
    - Software Defined Data Center (SDDC)
- Backup of Virtual Systems
    - Creating Backup of Virtual Machines Running on VMware
    - Backup Creation in Hyper-V

- Challenges in Virtualization Deployment
    - Network Connection
    - Creating excess VMs
    - Vendor-based Application Support
    - Cost
    - Security
- Best Practices in Virtualization
- Virtualization Standards
- Case Study

Module 09: System Recovery

- What is System Recovery?
- System Restore in Windows 10
- Linux System Recovery
    - Backup and Restoration of Ubuntu 16.04.1 (LTS)
- Mac System Recovery
    - Recovery
    - Time Machine Backup
- Restoration of Windows Server 2012
- Recovering from a Boot issue in Windows Server 2012 R2
    - Boot Manager Failure
    - Window Boots but Startup Fails
- Active Directory Recovery
    - Non-Authoritative Restoration
    - Authoritative Directory Restoration
- Verifying Active Directory Restoration
- Sysvol Recovery
    - Authoritative SYSVOL Restore
    - Non-Authoritative SYSVOL Restore
- Recovery of Global Catalog Servers
- Recovery of Domain Controller
- Database Integrity Testing
- Restoring IIS Configurations
- Restoring Microsoft IIS Metabase Backup
- Restoring Exchange Server 2016
    - Exchange Data Recovery Preparation
    - Single Mailbox Recovery

  - Single Item Recovery using Deleted Items Retention
  - Single Item Recovery using Third-party Brick Backup Programs
- IBM WebSphere Application Server Recovery
- Recovering from Domino Server Crashes
- Restoring MySQL Server

Module 10: Centralized and Decentralized System Recovery

- Introduction
- Centralized Computing
- Centralized Computing Architecture
  - Client-Server Architecture
  - Peer-to-Peer Architecture
  - Tightly Coupled Architecture
- Decentralized Computing
- Decentralized Computing Architecture
  - Peer-to-Peer Architecture
  - Loosely Coupled Architecture
- Differences between Centralized Computing and Decentralized Computing
- Survivable Storage Systems
  - What are Survivable Storage Systems?
  - PASIS Architecture

Module 11: Disaster Recovery Planning Process

- Introduction to Disaster Recovery (DR)
- Need for Disaster Recovery Planning
- Factors Affecting the Disaster Recovery (DR) Strategy
  - Technology
  - Data Criticality
  - Sites
  - People
  - Policies and Procedures
- Components of a Disaster Recovery Plan Strategy
  - Identifying Risks
  - Determining Threat Levels
  - Developing a Flexible Response Plan
  - Documenting the Recovery Approach
- Disaster Recovery Planning Process

    - Scope Statement
    - Exclusions
    - System Description
    - Interrogation
    - Activation Procedures
    - Execution Procedures
- DR Planning Methodology
    - Components of DR Planning Methodology
- Disaster Recovery Lifecycle
    - Reduce
    - Response
    - Recover
    - Re-sync
    - Resume
    - Return
- Tiers of Disaster Recovery
    - Tier 0: No Offsite Data
    - Tier 1: Data Backup without a Hot Site
    - Tier 2: Data Backup with a Hot Site
    - Tier 3: Electronic Vaulting
    - Tier 4: Point in Time Copies
    - Tier 5: Transaction Integrity
    - Tier 6: Zero or Near Zero Data Loss
    - Tier 7: Highly Automated Business Integrated Solution
- Data Protection and Recovery Strategy
- Establishing a Disaster Recovery Plan
    - Assumptions for Disaster Recovery Planning
    - Key DR Documentation Activities
    - Objectives of the Disaster Recovery Plan
    - Disaster Recovery and Management: Budgeting
- Develop a Disaster Recovery Team Structure
    - Disaster Recovery Team Organizational Structure
    - Disaster Recovery Sub-teams
- Disaster Recovery Plan Testing
    - Disaster Recovery Plan Testing Objectives
    - Scope, Assumptions, Criteria, and Life Cycle of Disaster Recovery Plan Testing

- DR Plan Testing Cycle
- DR Plan Implementation

Module 12: BCP Testing, Maintenance, and Training

- Business Continuity Plan Testing
- Elements of the BCP Test Plan
  - Orientation Test
  - Tabletop Test
  - Functional Test
  - Full-scale Test
- Maintaining the Business Continuity Plan
- Auditing the Business Continuity Plan
  - Overall Program Governance
  - Ongoing Program Management
  - Management of Change in Process
- BCP Training
- Implementing Business Continuity Training Program
- Establishing a BC Training Program
  - Awareness Training
  - Scenario Training
- Value of BC Training
  - Create a Competent Recovery Professional and Employee
  - Increase Plan Development Efficiency and Effectiveness
  - Integrate Risk Management Efforts
  - Grow Program Maturity
- BC Training Evaluation