Enterprise Network Disaster Recovery Planning Training Course

26 - 30 Oct 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #NO4050_118489

Course Introduction / Overview:

In today's hyper-connected digital landscape, the resilience of enterprise networks is not just an IT concern but a cornerstone of business survival and continuity. This course provides a comprehensive framework for developing, implementing, and managing a robust disaster recovery plan tailored for complex enterprise networks. We delve into the critical processes that safeguard an organization's network infrastructure against a wide range of disruptions, from cyber-attacks and hardware failures to natural disasters. As highlighted by the renowned expert Jon William Toigo in his seminal work, "Disaster Recovery Planning: Preparing for the Unthinkable," a proactive and well-tested plan is the only defense against catastrophic data loss and operational downtime. This program, offered by BIG BEN Training Center, moves beyond theoretical concepts to provide actionable strategies for conducting thorough risk assessments, performing business impact analyses, and establishing clear Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Participants will explore cutting-edge recovery technologies, including virtualization, cloud-based Disaster Recovery as a Service (DRaaS), and advanced data replication methods, ensuring their organizations can not only survive a disaster but recover with minimal impact on business operations, data integrity, and stakeholder confidence.

Target Audience / This training course is suitable for:

- IT Managers and Directors.
- Network Administrators and Engineers.
- Systems Administrators.
- Cybersecurity Analysts and Specialists.
- Business Continuity Planners.
- IT Auditors and Compliance Officers.
- Data Center Managers.
- Chief Information Officers (CIOs) and Chief Technology Officers (CTOs).
- Risk Management Professionals.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Telecommunications and IT Services.
- E-commerce and Retail.
- Manufacturing and Supply Chain.
- Energy and Utilities.
- Government Agencies and Public Sector Organizations.
- Education and Research Institutions.

Target Organizations Departments:

- Information Technology (IT) Department.
- Network Operations Center (NOC).
- Cybersecurity and Information Security.
- Operations Management.
- Risk Management and Compliance.
- Internal Audit.
- Facilities Management.
- Strategic Planning and Corporate Governance.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop a comprehensive disaster recovery plan for enterprise networks.
- Conduct a thorough business impact analysis (BIA) and risk assessment.
- Define and implement realistic Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Evaluate and select appropriate data backup and replication technologies.
- Design resilient network architectures that minimize single points of failure.
- Integrate cloud-based disaster recovery (DRaaS) solutions into their strategy.
- Establish clear roles, responsibilities, and communication protocols for the DR team.
- Plan and execute effective disaster recovery tests and drills.
- Maintain and update the DR plan to reflect changes in the IT environment.
- Align the network disaster recovery plan with the overall business continuity strategy.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to foster a dynamic and engaging learning environment that bridges theory with practical application. This course emphasizes an interactive, participant-centered approach, moving away from traditional lecture-based formats. Sessions will be facilitated through a blend of expert-led presentations, real-world case study analyses of major network outages, and collaborative group discussions. Participants will engage in hands-on workshops and simulation exercises where they will draft key components of a disaster recovery plan, conduct a mock business impact analysis, and debate strategic recovery options. This practical approach ensures that learners not only understand the concepts but can also apply them directly to their own organizational context. Ample time is allocated for Q&A sessions, peer-to-peer knowledge sharing, and personalized feedback from the instructor. The curriculum is structured to build skills progressively, ensuring a solid foundation before moving to more advanced topics, culminating in a comprehensive understanding of enterprise network resilience.

Course Agenda (Course Units):

Unit One: Foundations of Network Disaster Recovery

- Introduction to Business Continuity and Disaster Recovery.
- The high cost of network downtime and its impact on business.
- Differentiating between Business Continuity Planning (BCP) and Disaster Recovery (DR).
- Understanding key metrics: Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
- The Disaster Recovery lifecycle and its phases.
- Regulatory and compliance requirements for data and network availability.
- Establishing the scope and objectives of the DR plan.

Unit Two: Risk Assessment and Business Impact Analysis

- Identifying critical network assets and infrastructure components.
- Conducting a comprehensive Business Impact Analysis (BIA) for network services.
- Threat and vulnerability assessment for enterprise networks.
- Analyzing natural, technical, and man-made threats.
- Calculating the potential financial and operational impact of disruptions.
- Prioritizing network functions and applications for recovery.
- Documenting the findings of the BIA and risk assessment.

Unit Three: Designing Resilient Networks and DR Strategies

- Principles of high-availability network design.
- Implementing redundancy for core network components (routers, switches, firewalls).
- Exploring disaster recovery site options: hot, warm, and cold sites.
- Leveraging virtualization for rapid server and network recovery.
- Understanding data backup, replication, and snapshot technologies.
- Introduction to Cloud-based Disaster Recovery (DRaaS) models.
- Software-Defined Networking (SDN) in disaster recovery.

Unit Four: Developing and Documenting the DR Plan

- Structuring the official Disaster Recovery Plan document.
- Defining roles and responsibilities for the disaster recovery team.
- Creating step-by-step network recovery procedures.
- Developing a clear crisis communication plan for stakeholders.
- Vendor and service provider management during a disaster.
- Procedures for data restoration and integrity validation.
- Documenting emergency shutdown and failover processes.

Unit Five: Testing, Maintaining, and Activating the Plan

- The importance of regular DR plan testing.
- Types of disaster recovery tests: walkthrough, simulation, and full-interruption.
- Planning and executing a successful network DR drill.
- Analyzing test results and identifying gaps for improvement.
- Establishing a schedule for plan review and maintenance.
- Change management processes to keep the DR plan current.
- Incident response and plan activation procedures during a real disaster.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

In an era of increasingly sophisticated cyber-attacks and climate-related disruptions, how can an organization's disaster recovery plan evolve from a static document into a dynamic, adaptive framework for true enterprise resilience?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by moving beyond theoretical frameworks to provide a deeply practical and strategic perspective on enterprise network resilience. Unlike programs that focus solely on specific technologies or vendor solutions, our curriculum emphasizes the entire disaster recovery lifecycle, from initial risk assessment to post-incident review. A key differentiator is the strong focus on integrating network disaster recovery with broader business continuity and cybersecurity incident response strategies, a critical nexus often overlooked in standard training. Participants will not just learn what to do, but why they are doing it, by analyzing real-world case studies of catastrophic network failures and successful recoveries. The course content is continuously updated to address modern challenges, including the complexities of hybrid cloud environments, the role of Software-Defined Networking (SDN) in recovery, and the specific threats posed by ransomware. The methodology encourages critical thinking and problem-solving, equipping professionals with the strategic mindset needed to champion and manage a resilient DR program that truly supports and protects the business.