



Business Continuity, Disaster Recovery
Planning, and Risk Management



Business Continuity, Disaster Recovery Planning, and Risk Management

Introduction:

This program addresses the core of organizational resilience: advanced business continuity, enterprise-level account protection, disaster recovery engineering, and integrated risk management. The content is for professionals who need to design, stress-test, and maintain systems that stay operational under pressure, adapt fast, and recover without losing data, customers, or credibility.

By the end of this course, participants will have a rock-solid understanding of resilience frameworks, continuity engineering, crisis response modeling, and integrated risk governance for organizational accounts and operations.

Targeted Groups:

- Business Continuity Managers.
- Risk & Compliance Officers.
- IT Disaster Recovery Engineers.
- Operations Leaders.
- Enterprise Account Managers.
- Data Security & IT Governance Professionals.
- Internal Audit Teams.
- Crisis Management Teams.

Training Course Objectives:

By the end of this program, participants will be able to:

- Build enterprise-grade continuity and recovery plans.
- Conduct impact analysis tied specifically to business accounts and operational dependencies.
- Architect disaster recovery processes aligned with industry standards.
- Identify, measure, and mitigate high-value account risks.
- Establish governance, reporting, and audit cycles for resilience programs.
- Evaluate vendor and third-party risk exposure.
- Design escalation and communication structures for crisis scenarios.

Targeted Competencies:

- Strategic risk analysis.
- Business impact assessment.
- Technical disaster recovery design.
- Regulatory alignment and compliance.
- Crisis leadership and decision-making.
- Cross-functional coordination.
- Incident lifecycle management.
- Documentation and governance discipline.

Course Content:

Unit 1: Advanced Business Continuity Foundations:

- The evolution of business continuity in complex and high-dependency organizations.
- Continuity frameworks aligned to critical enterprise accounts and revenue streams.
- The relationship between continuity, resilience, and operational discipline.
- Mapping organizational assets, workflows, and interdependencies.
- Identifying continuity blind spots: manual workarounds, undocumented processes, legacy systems.
- Lifecycle of the Business Continuity Management System BCMS.
- Policy development, governance layers, and accountability models.

Unit 2: Business Impact Analysis & Criticality Modeling:

- Deep-dive Business Impact Analysis BIA methodologies.
- Evaluating financial, operational, legal, reputational, and customer-side impact.
- Aligning BIA outcomes with enterprise accounts and service-level obligations.
- Critical function mapping and process interdependency analysis.
- Recovery Time Objectives RTO and Recovery Point Objectives RPO: advanced configuration.
- Prioritizing resource allocation for high-value accounts.
- Modeling downtime scenarios using quantitative and qualitative assessment tools.
- Translating BIA findings into executive-ready reports and continuity strategies.

Unit 3: Disaster Recovery Architecture & Execution:

- Advanced disaster recovery DR frameworks and architectures.
- Technical replication strategies: synchronous, asynchronous, point-in-time.
- Failover engineering across cloud, hybrid, and on-premise environments.
- DR for enterprise accounts: data integrity, access management, and system dependencies.
- DR testing methodologies: tabletop, simulation, complete failover, and automated orchestration.
- Building multi-region, multi-site resilience.
- Backup lifecycle management and long-term preservation of critical data.
- Metrics and KPIs for DR program maturity.

Unit 4: Enterprise Risk Management & Operational Risk Controls:

- Integrated Risk Management IRM principles for large organizations.
- Risk appetite, tolerance, and thresholds for critical accounts.
- Risk identification frameworks: internal, external, systemic, cascading.
- Quantitative and qualitative risk scoring.
- Building risk registers and mapping risk ownership.
- Controls design: preventative, detective, corrective, and compensating.
- Monitoring, testing, and validating control effectiveness.
- Regulatory compliance requirements tied to continuity and DR.
- Reporting risk exposure to executive and board-level committees.

Unit 5: Crisis Management, Communication, and Continuous Improvement:

- Designing a functional crisis management structure.
- Incident lifecycle: detection, escalation, response, containment, recovery.
- Command center structure and leadership protocols.
- Internal and external communication strategies during crises.
- Customer communication frameworks for high-value accounts.
- Lessons learned, methodology, and after-action reporting.
- Continuous improvement loops for BCP, DR, and risk programs.
- Maturity models: measuring resilience growth over time.
- Exercises, simulations, and cross-team coordination cycles.