CONCEPT

IT Disaster Recovery Planning and Operational Resilience

IT Disaster Recovery Planning and Operational Resilience

Technical depth: Practitioner · **Practical mode:** Simulation

Introduction

Ransomware, cloud outages and data centre failures now halt entire business services, and many IT recovery plans rely on backups that cannot be restored, sequences never rehearsed and providers never assessed. Boards and auditors increasingly ask whether important services can stay within tolerable disruption, not whether a recovery document exists. This Core Concept course equips IT and resilience managers to design, document and test recovery capability against international standards. Participants rehearse recovery decisions in time-pressured simulations and leave with an IT Disaster Recovery Plan and Resilience Test Schedule for a critical service.

Course Objectives

- Identify important business services and map the technology, data and third-party dependencies behind them
- Apply ISO/IEC 27031 and NIST SP 800-34 to structure an ICT readiness and contingency programme
- Select recovery architectures and backup strategies that meet agreed recovery time and recovery point objectives
- Write executable recovery runbooks, roles and declaration criteria, including for cyber attacks
- Plan and evaluate recovery tests, provider resilience reviews and post-incident remediation
- Produce an IT Disaster Recovery Plan and Resilience Test Schedule for a critical service

Target Audience

- IT infrastructure and operations managers accountable for platform availability
- Disaster recovery and IT service continuity managers
- Information security managers responsible for incident recovery and backup assurance
- Cloud and data centre managers overseeing hosting and failover arrangements
- IT risk and operational resilience managers reporting on recovery capability
- Application and service owners accountable for critical business systems

Course Outline

Day 1: IT Recovery and Operational Resilience Foundations

- Important Business Services and Impact Tolerance Concepts
- BCBS Principles for Operational Resilience Overview
- IT Service Dependency Mapping: Applications, Infrastructure, Data and Third Parties
- Disruption Scenario Catalogue: Ransomware, Site Loss, Cloud Region Outage and Supplier Failure
- Recovery Capability Baseline Assessment Checklist

Day 2: Standards and Recovery Architecture

- ISO/IEC 27031:2025 ICT Readiness for Business Continuity
- NIST SP 800-34 Contingency Planning Process
- ISO/IEC 27001:2022 Controls 5.30, 8.13 and 8.14 for ICT Continuity, Backup and Redundancy
- ITIL 4 Service Continuity Management Practice
- Recovery Architecture Patterns: Backup and Restore, Pilot Light, Warm Standby and Active-Active

Day 3: Building the Recovery Capability

- Recovery Objective Alignment: RTO, RPO and Recovery Sequence by Service
- Backup Strategy Design with the 3-2-1-1-0 Rule and Immutable Copies
- Runbook Writing for Failover, Failback and Data Restoration
- Recovery Roles, Call Trees and Disaster Declaration Criteria
- Cyber Recovery Planning with the NIST CSF 2.0 Recover Function and SP 800-184

Day 4: Testing, Provider Risk and Optimisation

- Recovery Test Types: Walkthrough, Component Restore, Parallel and Full Interruption
- Chaos Engineering and Controlled Failure Injection
- Cloud and Outsourced Provider Resilience Due Diligence and Exit Plans
- Recovery Metrics: Test Success Rate, Achieved Recovery Time and Measured Data Loss
- Post-Incident Review and Remediation Tracking Log

Day 5: Simulation and the IT Disaster Recovery Plan

- Ransomware Recovery Simulation: Clean Environment Restore Decisions
- Site Loss Simulation: Failover Sequencing Under Time Pressure
- Simulation Debrief Against Impact Tolerances
- IT Disaster Recovery Plan Drafting for an Own Critical Service
- Resilience Test Schedule Build and Peer Review

Skills You Will Gain

- Service Dependency Mapping
- Recovery Architecture Selection
- Backup Strategy Design
- Recovery Runbook Development
- Cyber Recovery Planning
- Recovery Test Management
- Provider Resilience Assessment
- Impact Tolerance Setting

Why Attend This Course

- Return with an IT Disaster Recovery Plan and Resilience Test Schedule for a critical service, reviewed by peers
- Experience recovery decisions under time pressure before facing them in a real outage
- Give business owners, auditors and boards evidence that recovery objectives can actually be met
- Learn from infrastructure and security managers in banking, telecoms, government and industry

Conclusion

Recovery capability is proved only by restoring services within agreed limits. This course moves from important business services and dependency mapping, through ICT readiness standards and recovery architectures, to runbooks, backup design, cyber recovery, testing and provider resilience. The final day places participants in ransomware and site loss simulations and turns the lessons into an IT Disaster Recovery Plan and Resilience Test Schedule, giving them a tested basis for showing that critical services can be recovered when it matters.