

Strategic Disaster Recovery & Business Continuity for IT Professionals

Training Overview:

This 5-day course equips IT professionals and functional leaders with a comprehensive approach to Disaster Recovery (DR) through the lens of Business Continuity (BC), using the BCI lifecycle.

Training Objectives:

By the end of this course, participants will:

1. Apply the BCI lifecycle to disaster recovery and crisis planning
2. Conduct a risk-informed Business Impact Analysis with IT asset focus
3. Design DR strategies involving backup, cloud, systems, and applications
4. Integrate DR testing, auditing, and improvement cycles
5. Manage communications and decision-making during crises
6. Collaborate across business and IT teams in continuity planning

Target Audience:

- IT professionals responsible for resilience and recovery
- Project managers in tech environments
- Functional leaders collaborating with IT on BCM

Course Structure

Each day = 1 BCI Lifecycle Phase + Embedded IT DR Focus

Training Duration

5 Days

Training Gamification

- Crisis Simulation Scenarios – Teams respond to real-time disaster events with DR/BC strategies under pressure.
- Tech Translator Challenge – Participants simplify complex IT concepts for non-technical stakeholders.
- Command Roleplay (Gold/Silver/Bronze) – Rotating leadership roles during crisis simulations to drive decision-making.
- Leaderboard & Badges – Points awarded daily with visible rankings and titles like “BCM Champion” or “DR Strategist.”
- Case Study Design Battle – Final team challenge to create and defend a full DR/BC plan for a complex business case.

Training Outlines

Day 1: POLICY & PROGRAM – Foundations of BCM & IT DR

- What is BC, DR, Crisis? Differences and links
- The BCI Lifecycle + ISO 22301
- Governance structure for BCM
- Setting DR policy across IT systems (roles, tiers, ownership)
-  Simulation: Draft your DR Policy & Escalation Chart
-  IT Angle: Define system tiers (Tier 1–3), DR policies per system type

Day 2: BIA – Impact, Dependencies & IT Systems

- Business Impact Analysis methodology (MTPD, RTO, RPO)
- Asset prioritization (critical apps, infra, data, people)
- Mapping dependencies: upstream & downstream
-  Workshop: Create BIA matrix for a hybrid IT company
-  IT Angle: How to calculate RTO/RPO per system (database vs cloud vs mobile)

Day 3: STRATEGY – DR Solutions Design & Crisis Planning

- Strategy options: work-area recovery, cloud failover, split-site
- DR plans by function: storage, apps, networks, people
- Crisis communication principles (inside IT, outside org)
-  Activity: Design a DR response to a ransomware attack
-  IT Angle: Match DR tech (RAID, VM snapshots, DRaaS) to business strategy

Day 4: RESPONSE STRUCTURES – Crisis Teams, Plans, and Exercises

- Gold/Silver/Bronze command structure
- DR Plans & Crisis Playbooks
- Exercise types: tabletop, simulation, full-scale
-  Scenario: Earthquake strikes — activate crisis team, run comms, simulate failover

-  IT Angle: DR testing checklist (backup verification, failover, restore validation)

Day 5: MAINTENANCE & AUDIT – Sustaining DR Performance

- Continuous improvement in BCM/DR
- DR audits and compliance (ISO, NIST, regulators)
- Documentation essentials: Logs, SOPs, contact trees
-  Final Challenge: Deliver a DR walkthrough (team-based)
-  IT Angle: Audit sample – Is your DR plan technically sound?