JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced IT Disaster Recovery and Business Continuity Training Course

4 – 15 July 2027
Kuala Lumpur

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced IT Disaster Recovery and Business Continuity Training Course

Ref: 172_4968 **Date:** 4 – 15 July 2027 **Location:** Kuala Lumpur **Fees:** 8000 GBP

Advanced IT Disaster Recovery and Business Continuity is a 2-week training course for IT disaster recovery managers, infrastructure leads and continuity coordinators, built around a set of disaster recovery runbooks that each participant completes and shares with colleagues. Ransomware, cloud concentration and always-on digital services mean that an infrastructure outage now halts revenue and public services within minutes. Jupiter Prime Training offers IT Disaster Recovery and Business Continuity for those who keep systems recoverable.

Why IT Disaster Recovery and Business Continuity Matter Now

Three forces shape technology recovery today: destructive cyber attacks that encrypt or corrupt backups as well as production systems, hybrid estates that spread workloads across on-premises data centres and several cloud providers, and business owners who expect digital services to return within agreed windows. A bank whose payment platform fails, or a hospital whose patient records become unavailable, faces harm to people as well as finances. Teams that tie recovery architecture to business priorities restore what matters first; teams that rely on untested failover discover gaps during the outage. The course connects technology recovery to ISO 22301, the international standard for business continuity management systems BCMS.

Who Gains Most from IT Disaster Recovery and Business Continuity

- Leaders accountable for recovery capability across data centres and cloud platforms
- Infrastructure and platform heads who design backup, replication and failover arrangements
- Security operations leads who coordinate cyber incident containment with system restoration
- Continuity coordinators who translate business recovery needs into technology requirements
- Service owners who approve recovery sequences for critical applications

A technology function gains most when its recovery manager, a cloud architect and a security operations lead attend together and agree how restoration and containment interact.

IT Disaster Recovery and Business Continuity Capabilities

Participants leave able to design, test and document technology recovery that matches what the business can tolerate.

- Specify recovery time and recovery point targets per application tier — service owners and continuity coordinators
- Design backup, replication and failover architecture for hybrid estates — infrastructure investment decisions
- Build immutable and isolated backup arrangements — cyber resilience and security operations
- Test failover and failback through staged exercises — assurance for technology executives
- Weigh data centre, colocation and cloud recovery options — cost and contract decisions
- Communicate recovery status and residual gaps — business owners and executive committees

Key IT Disaster Recovery and Business Continuity Terms

- Recovery time objective RTO — the maximum target time to restore a system or application after an outage.
- Recovery point objective RPO — the maximum acceptable age of restored data, defining how much recent information may be lost.
- Replication — copying data continuously or periodically to another site or platform so it can take over when needed.
- Failover — switching processing from a failed system to a standby system, followed later by failback to the original.
- Immutable backup — a backup copy that cannot be altered or deleted for a set period, protecting it from ransomware.
- Disaster recovery runbook — a step-by-step technical procedure for restoring a specific system, with owners, dependencies and checks.

IT Disaster Recovery and Business Continuity Day by Day

Day 1: Technology Recovery in Context

- ISO 22301 Continuity Requirements — Linking Technology Recovery to Business Priorities
- Digital Service Dependency Mapping — Tracing Applications, Infrastructure and Third Parties
- Outage Scenario Catalogue — Comparing Hardware, Site, Cloud and Cyber Failures
- Recovery Maturity Assessment — Prioritising Gaps Across the Technology Estate
- Banking and Healthcare Outage Cases — Drawing Lessons From Prolonged Service Loss

Day 2: Recovery Objectives for Technology

- Application Tiering Model — Grouping Systems by Business Criticality
- RTO and RPO Derivation — Translating Business Tolerance Into Technical Targets
- Recovery Sequence Planning — Ordering Restoration Around Shared Dependencies
- Gap Analysis Against Current Capability — Exposing Unrealistic Recovery Promises
- Objective Sign-Off With Service Owners — Agreeing Targets Before Investment

Day 3: Backup and Data Protection Architecture

- Backup Strategy Patterns — Choosing Full, Incremental and Snapshot Approaches
- Three-Copy, Two-Media, One-Offsite Principle — Diversifying Backup Locations
- Immutable and Isolated Backups — Protecting Copies From Ransomware and Insiders
- Restore Validation Routines — Proving Backups Can Actually Be Recovered
- Retention and Encryption Settings — Balancing Recovery Needs With Data Protection

Day 4: Replication and High Availability

- Synchronous Versus Asynchronous Replication — Trading Data Loss Against Distance and Cost
- Database Replication Options — Protecting Transactional Integrity During Failover
- Active-Active and Active-Passive Designs — Choosing Availability Patterns per Tier
- Network and DNS Failover — Redirecting Users to Recovered Services
- Single Point of Failure Review — Removing Hidden Weaknesses in Infrastructure

Day 5: Data Centre, Colocation and Cloud Recovery

- Secondary Data Centre Options — Weighing Owned, Shared and Colocation Sites
- Cloud Recovery Patterns — Using Pilot Light, Warm Standby and Multi-Region Designs
- Disaster Recovery as a Service Evaluation — Assessing Provider Capability and Contracts
- Cloud Concentration Exposure — Managing Dependence on a Single Provider
- Recovery Cost Modelling — Comparing Standby Costs With Outage Losses

Day 6: Cyber Incident Recovery

- Ransomware Recovery Sequence — Isolating, Cleaning and Restoring in Order
- Clean Room Recovery Environment — Rebuilding Trusted Systems Away From Infection
- Identity and Directory Restoration — Re-Establishing Trusted Access First
- Forensic Evidence Preservation — Balancing Investigation Needs With Restoration Speed
- Security and Recovery Team Coordination — Aligning Containment With Service Restoration

Day 7: Disaster Recovery Runbooks

- Runbook Structure Standard — Writing Steps, Owners, Prerequisites and Verification Checks
- Automation of Recovery Steps — Reducing Manual Error During Restoration
- Dependency Start-Up Order — Sequencing Infrastructure, Middleware and Applications
- Runbook Version Control — Keeping Procedures Aligned With Changing Systems
- Offline Runbook Access — Ensuring Procedures Remain Available During Outages

Day 8: Failover Testing and Exercising

- Test Types Ladder — Progressing From Component Restores to Full Site Failover
- Test Planning and Change Control — Protecting Production While Proving Recovery
- Failback Procedures — Returning Safely to Primary Systems
- Test Evidence and Metrics — Measuring Achieved Recovery Times Against Targets
- Remediation Tracking — Closing Weaknesses Found in Recovery Tests

Day 9: Recovery Oversight and Supplier Assurance

- Technology Recovery Policy — Defining Ownership, Standards and Review Cycles
- Change Management Integration — Updating Recovery Designs When Systems Change
- Supplier and Cloud Provider Assurance — Verifying Contractual Recovery Commitments
- Recovery Readiness Dashboard — Reporting Status to Executives and Service Owners
- Continuity Coordination Interface — Aligning Technology Recovery With Business Plans

Day 10: Practising the Disaster Recovery Runbooks

- Ransomware Recovery Simulation — Applying Clean Room and Restore Sequences
- Regional Outage Failover Exercise — Testing Replication and Network Redirection
- Recovery Objective Verification — Comparing Achieved Times With Agreed Targets
- Peer Review of Runbooks — Refining Steps, Owners and Verification Checks
- Disaster Recovery Runbooks — Assembling Tiering, Architecture, Procedures and Test Evidence

Applying IT Disaster Recovery and Business Continuity After the Course

- Lead a restore validation test for the three most critical applications and record achieved recovery times against agreed targets.
- Review backup isolation and immutability settings with the security operations team and close any copy reachable from production credentials.

IT Disaster Recovery and Business Continuity Questions FAQ

What is IT disaster recovery and business continuity and why does it matter now?

IT disaster recovery and business continuity is the discipline of restoring technology services within targets the business can tolerate. It matters now because ransomware, cloud concentration and always-on digital services turn infrastructure outages into immediate operational and financial harm.

Which roles gain most from advanced IT disaster recovery and business continuity?

Disaster recovery managers, infrastructure and cloud leads, security operations leads and continuity coordinators gain most. You benefit if you design backup or replication, write recovery procedures, or report technology readiness to service owners.

How does advanced IT disaster recovery and business continuity differ from a business continuity planning course?

Advanced IT disaster recovery and business continuity focuses on technology architecture, replication, cyber recovery and runbooks. A business continuity planning course concentrates on impact analysis, business strategies and governance, while this one delivers the technical recovery those plans depend on.

What do you bring back from IT disaster recovery and business continuity training?

You bring back a set of disaster recovery runbooks with application tiering, recovery targets, architecture choices and test evidence. They give your technology team tested procedures to follow during the next serious outage.

IT Disaster Recovery and Business Continuity: The Way Forward

The disaster recovery runbooks give a technology function documented, tested routes back to service for its critical systems. Their first use is confirming the restoration order for shared infrastructure such as identity and networking. Recovery managers, platform engineers and security operations use them together. After the first full failover test, the recovery point targets deserve another look, since replication lag often differs from design assumptions.