

Schedule

Date	Venue	Fees (Face-to-Face)
10 - 14 Aug 2026	London, UK	USD 3495 per delegate

► Available delivery methods: Face-to-Face & Online Training

Introduction

Disaster recovery is critical to maintaining operational continuity in the face of natural, technological, or human-made disruptions. However, having a plan is not enough—it must be auditable, effective, and continually improved. This course equips professionals with the knowledge and tools to assess the adequacy and performance of an organization’s disaster recovery (DR) capabilities. Participants will learn to evaluate DR policies, procedures, infrastructure, and readiness through an auditor’s lens. By the end of the course, they will be able to conduct a structured disaster recovery audit that identifies vulnerabilities, tests recovery procedures, and supports organizational resilience objectives.

Objectives

- By the end of this course, participants will be able to:
- Understand disaster recovery frameworks and their audit relevance
 - Evaluate the effectiveness and readiness of disaster recovery plans
 - Identify gaps and risks in IT recovery capabilities and infrastructure
 - Develop audit programs tailored to DR planning and testing
 - Recommend improvements based on audit evidence and risk assessment

Why Attend

- Learn how to audit disaster recovery plans using globally accepted standards
- Improve your organization's resilience posture and audit preparedness
- Understand key controls and metrics for DR plan effectiveness
- Gain hands-on skills for assessing technical recovery and business continuity alignment
- Enhance the value of internal audit through a risk-based DR audit approach

Target Audience

This program is designed for:

- IT auditors and internal auditors
- Disaster recovery and business continuity professionals
- IT risk and compliance managers
- Information security officers
- Consultants assessing DR and continuity controls

Individual Benefits

Key competencies that will be developed include:

- Knowledge of disaster recovery standards (ISO 22301, ISO 27031, NIST)
- Ability to assess recovery readiness, RTOs/RPOs, and test results
- Proficiency in auditing DR documentation, infrastructure, and procedures
- Enhanced risk assessment and control evaluation capabilities
- Confidence in reporting findings to executive leadership

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved resilience through effective disaster recovery audits
- Enhanced ability to identify recovery risks before disruptions occur
- Stronger alignment between DR strategy, technology, and business priorities
- Support for regulatory compliance and IT governance frameworks
- Greater assurance to stakeholders on recovery preparedness

Instructional Methodology

The course follows a blended learning approach combining theory with practice:

- Strategy Briefings – Deep dive into disaster recovery frameworks, standards, and audit processes
- Case Studies – Real-world examples of disaster recovery audit successes and failures
- Workshops – Hands-on activities to audit DR plans, test results, and documentation
- Peer Exchange – Discussions on audit challenges, regulatory trends, and incident responses
- Tools – Templates for DR audit checklists, evaluation frameworks, and reporting

Course Outline

Training Hours: 7:30 AM – 3:30 PM **Daily Format:** 3–4 Learning Modules | Coffee breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00

Day 1: Foundations of Disaster Recovery and Auditing

- Module 1: Introduction to Disaster Recovery and BCM (07:30 – 09:30)
- Overview of disaster recovery and its relationship with business continuity
- Key DR concepts: RTO, RPO, recovery tiers, backup strategies
- Regulatory and industry frameworks (ISO 22301, ISO 27031, COBIT, NIST)
- Module 2: DR Audit Fundamentals (09:45 – 11:15)
- Purpose and scope of disaster recovery audits
- The auditor's role in resilience assurance
- Risk-based auditing and audit lifecycle
- Module 3: DR Policy and Governance Review (11:30 – 01:00)
- Evaluating DR policies and recovery strategy alignment
- Roles, responsibilities, and organizational structure
- Policy effectiveness and governance metrics
- Module 4: Workshop – Readiness Checklist Evaluation (02:00 – 03:30)
- Develop a disaster recovery audit readiness checklist
- Review a sample DR policy for completeness and controls
- Peer feedback on policy audit results

Day 2: Risk Assessment and DR Infrastructure Review

- Module 1: Risk and Impact Assessments (07:30 – 09:30)
- Conducting Business Impact Analysis (BIA) for audit context
- Risk assessment techniques for recovery planning
- Mapping critical processes and IT dependencies
- Module 2: DR Infrastructure Components (09:45 – 11:15)
- Key components of DR infrastructure: backups, alternate sites, cloud, etc.
- Evaluating redundancy, failover, and restoration capabilities
- Reviewing infrastructure configurations and documentation
- Module 3: Testing and Maintenance Audit (11:30 – 01:00)
- Types of disaster recovery tests: tabletop, simulation, full interruption
- Evaluating test plans, outcomes, and lessons learned
- Maintenance frequency and audit evidence collection
- Module 4: Workshop – Reviewing a DR Test Plan (02:00 – 03:30)
- Analyze a real test plan for coverage and effectiveness
- Identify audit findings and potential improvements
- Document audit results in standard format

Day 3: Application, Data, and Network Recovery Audits

- Module 1: Application Recovery Evaluation (07:30 – 09:30)
- Auditing mission-critical application recovery
- Recovery priorities and interdependencies
- Review of application backup procedures
-

Module 2: Data Backup and Restoration Controls (09:45 – 11:15)

- Reviewing backup policies and frequency
- Evaluating encryption, integrity, and offsite storage
- Sample audit of backup logs and recovery drills
- Module 3: Network and Communications Continuity (11:30 – 01:00)
- Assessing communication plans and escalation procedures
- Reviewing network resilience, VPNs, and cloud continuity
- Role of IT support and remote access in DR
- Module 4: Workshop – System Recovery Audit Simulation (02:00 – 03:30)
- Evaluate an end-to-end recovery scenario
- Simulate audit steps and prepare findings
- Present audit results and get feedback

Day 4: Integrating DR Audits with Business Continuity and Cybersecurity

- Module 1: DR vs. BCM: Integration and Differences (07:30 – 09:30)
- Integrating DR with broader business continuity management
- Communication and coordination during crises
- Audit synergy between BCP and DRP
- Module 2: Cybersecurity and Disaster Recovery (09:45 – 11:15)
- Cyber incidents as triggers for DR
- Auditing cyber recovery controls and response plans
- DR audit readiness in a cyberattack environment
- Module 3: DR Documentation and Reporting (11:30 – 01:00)
- Key audit deliverables and documentation standards
- Writing impactful DR audit reports
- Audit committee and executive communication
- Module 4: Workshop – Risk-Based Audit Program Design (02:00 – 03:30)
- Design a customized DR audit plan
- Align objectives, risks, and controls
- Peer review and improvement suggestions

Day 5: Capstone Case Study and Course Wrap-Up

- Module 1: Ethics and Professional Considerations (07:30 – 09:30)
- Ethical responsibilities of DR auditors
- Confidentiality, independence, and audit integrity
- Addressing audit conflicts professionally
- Module 2: Case Study – DR Audit in Practice (09:45 – 11:15)
- Analyze a real-world DR failure and audit trail
- Identify missed audit opportunities and risks
- Extract best practices from post-audit reviews
- Module 3: Capstone Exercise – Full DR Audit Simulation (11:30 – 01:00)
- Conduct a simulated DR audit based on provided scenario
- Audit planning, execution, findings, and recommendations
- Present results to the group for critique
- Module 4: Final Summary and Certification (02:00 – 03:30)

- Key takeaways from the course
- Review of tools and techniques
 - Awarding of certificates and closure

Certification

Participants will receive a Certificate of Completion in Disaster Recovery Audit, affirming their ability to assess, review, and improve disaster recovery plans in alignment with best practices and resilience standards.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation’s unique goals.

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: +601116373203	EMAIL: info@mawaevents.net
---	----------------------------------	--

© Material published by MAWA Events shown here is copyrighted. All rights reserved. Any unauthorized copying, distribution, use, dissemination, downloading, storing (in any medium), transmission, reproduction or reliance in whole or any part of this course outline is prohibited and will constitute an infringement of copyright.