

PATCH MANAGEMENT AUDIT: ENSURES THAT SYSTEMS ARE REGULARLY UPDATED WITH THE LATEST SECURITY PATCHES

“Ensure Every System Stays Secure, Up-to-Date, and Audit-Ready”

Schedule

Date	Venue	Fees (Face-to-Face)
23 – 27 Mar 2026	London – UK	USD 3,495 per delegate

► **Available delivery methods:** In-House Training

Introduction

In the face of relentless cyber-threats and tightening compliance mandates, timely patching is mission-critical. Yet many organisations still struggle to track, test, deploy, and verify security updates across diverse environments. This intensive five-day programme arms IT auditors, security leaders, and operations teams with proven frameworks and hands-on skills to evaluate, improve, and continuously monitor enterprise patch-management processes in line with global standards and best practice.

Objectives

- By the end of the course participants will be able to:
- Interpret patch-management requirements in ISO 27001, NIST SP 800-40, CIS, PCI-DSS, and SOC 2.
 - Map the full patch lifecycle—from vulnerability discovery to deployment validation.
 - Design audit scopes, criteria, and evidence-collection plans for patch compliance.
 - Use industry tools (e.g., WSUS, SCCM/MECM, Intune, Tanium, Qualys, Nessus) to verify coverage and remediate gaps.
 - Quantify patch-related risk and communicate findings to technical and executive stakeholders.
 - Draft actionable audit reports that drive measurable improvements.

Why Attend

- Mitigate risk of exploits that target unpatched systems.
- Prove compliance to regulators, clients, and external auditors.
- Optimise resources by identifying bottlenecks in current patch processes.
- Enhance career prospects with specialised IT-audit capabilities.
- Network & benchmark with peers facing similar security challenges.

Target Audience

This program is designed for:

- Business continuity managers and professionals responsible for BCP implementation
- Risk management and compliance officers
- IT disaster recovery specialists
- Operations and facility managers
- Senior management and executives overseeing business resilience
- Internal auditors and consultants

Individual Benefits

Key competencies that will be developed include:

- Proficiency in ISO 22301:2019 structure and implementation
- Capability to conduct BIAs and continuity risk assessments
- Skills to design and maintain continuity and crisis response plans
- Knowledge of performance evaluation, audit, and continuous improvement in BCMS
- Strategic planning for business resilience and recovery

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Enhanced organizational resilience and preparedness
- Stronger alignment with global business continuity best practices
- Improved risk management and reduced downtime from disruptions
- Documented continuity strategies enhancing stakeholder confidence
- Readiness for ISO 22301:2019 certification audits

Instructional Methodology

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

- Strategy Briefings – Deep dive into ISO 22301:2019, business continuity management principles, and BCMS frameworks
- Case Studies – Real-world examples of successful BCMS implementation and crisis response
- Workshops – Hands-on exercises to create business continuity plans, risk assessments, and recovery strategies
- Peer Exchange – Group discussions on challenges and lessons learned in business continuity
- Tools – Templates for BIA, risk assessments, business continuity plans, and crisis communication

Course Outline

Detailed 5-Day 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: Introduction to ISO 22301:2019 and Business Continuity Planning

- Module 1: Overview of ISO 22301:2019 (07:30 – 09:30)
- Introduction to ISO 22301:2019 and its importance in business continuity management
- Key principles and requirements of ISO 22301:2019
- Overview of the BCMS lifecycle and its role in organizational resilience
- Module 2: Business Continuity Concepts and Governance (09:45 – 11:15)
- Definitions and core components of a BCMS
- Leadership and governance roles in business continuity
- Integration with organizational strategy
- Module 3: Policy, Scope, and Objectives (11:30 – 01:00)
- Establishing scope and context of the BCMS
- Setting objectives and continuity policy aligned with ISO 22301
- Module 4: Risk Management Fundamentals (02:00 – 03:30)
- Risk identification and mitigation strategies
- Relationship between risk management and business continuity

Day 2: Business Impact Analysis (BIA) and Risk Assessment

- Module 5: Conducting a Business Impact Analysis (07:30 – 09:30)
- Purpose and process of BIA
- Identifying critical functions and acceptable downtime
- Module 6: Risk Assessment Methodology (09:45 – 11:15)
- Analyzing continuity risks and vulnerabilities
- Evaluating likelihood and impact
- Module 7: BIA & RA Workshops (11:30 – 01:00)
- Hands-on session using BIA and RA templates
- Module 8: Strategy Development (02:00 – 03:30)
- Developing continuity and recovery strategies
- Linking risks and BIA findings to mitigation planning

Day 3: Designing and Implementing the BCMS

- Module 9: Resource Planning and Documentation (07:30 – 09:30)
- Allocating resources and responsibilities for BCMS implementation
- Document control and version management
- Module 10: Business Continuity Plan Development (09:45 – 11:15)
- Elements of a strong business continuity plan
- Continuity planning for departments, processes, and systems
- Module 11: Crisis Communication Planning (11:30 – 01:00)
- Developing internal and external communication strategies
- Notification protocols and escalation paths
- Module 12: Workshop – Creating a Business Continuity Plan (02:00 – 03:30)

Day 4: Testing, Exercising, and Monitoring the BCMS

- Module 13: Testing and Exercising Plans (07:30 – 09:30)
- Types of continuity exercises (table-top, simulations, full-scale drills)
- Designing and evaluating test outcomes
- Module 14: Monitoring and Performance Evaluation (09:45 – 11:15)
- ISO 22301 metrics and KPIs
- Management reviews and performance tracking
- Module 15: Internal Audit of BCMS (11:30 – 01:00)
- Planning and executing BCMS internal audits
- Addressing nonconformities and corrective actions
- Module 16: Workshop – Continuity Exercise Design (02:00 – 03:30)

Day 5: Certification, Improvement & Course Review

- Module 17: Preparing for ISO 22301 Certification (07:30 – 09:30)
- Certification requirements and audit process
- Role of external auditors and registrar bodies
- Module 18: Continuous Improvement of BCMS (09:45 – 11:15)
- Root cause analysis and process improvements
- PDCA cycle for resilience enhancement
- Module 19: Final Assessment and Group Activity (11:30 – 01:00)
- Review quiz and team presentation on continuity planning
- Module 20: Course Wrap-Up and Feedback (02:00 – 03:30)
- Key takeaways, Q&A, and certificate distribution

Certification

Upon successful completion, delegates receive a Certificate of Completion – Patch Management Audit (Advanced), affirming their capability to assess, report, and strengthen enterprise patch-management practices in line with leading security and audit 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

Follow us:  Facebook  Twitter  YouTube  LinkedIn  Instagram

© 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.