MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

EFFECTIVE INFORMATION SECURITY AUDIT

""Auditing Information Systems to Strengthen Data Protection, Risk Management & Cybersecurity Compliance""

Schedule

Date	Venue	Fees (Face-to-Face)
07 – 11 Sep 2026	London, UK	USD 3495 per delegate

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

Introduction

In an era of escalating cyber threats, regulatory scrutiny, and business dependence on digital infrastructure, organizations must proactively assess the effectiveness of their information security controls. An information security audit provides assurance that systems, policies, and practices meet internal standards and comply with regulations like ISO/IEC 27001, GDPR, and NIST.

This intensive 5-day course equips internal auditors, IT professionals, and risk managers with the knowledge, tools, and techniques to plan and execute comprehensive information security audits. Participants will gain hands-on experience auditing governance frameworks, technical controls, access management, and incident response mechanisms.

Objectives

By the end of this course, participants will be able to:

- Understand the principles, scope, and methodology of information security auditing
- Plan and conduct risk-based audits of IT environments and ISMS controls
- Evaluate compliance with ISO 27001, cybersecurity frameworks, and privacy laws
- Identify control weaknesses and recommend practical improvements
- Prepare audit reports that support decision-making and regulatory readiness

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Why Attend

- To ensure your organization’s information security controls are effective and compliant
- To detect and address gaps in access, encryption, policies, and monitoring
- To support certification readiness for standards like ISO 27001
- To reduce exposure to cyber risk and data breaches
- To build internal audit capacity in information and cybersecurity governance

Target Audience

This program is designed for:

- Internal and IT auditors
- Information security officers and cybersecurity managers
- Compliance, risk, and data privacy professionals
- IT operations and infrastructure managers
- Anyone responsible for evaluating information security controls

Individual Benefits

Key competencies that will be developed include:

- ISMS auditing and evidence-based assessment
- IT risk and vulnerability analysis
- Control testing and documentation review
- Compliance mapping to ISO 27001, GDPR, NIST CSF
- Reporting, recommendations, and audit follow-up

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved risk awareness and cybersecurity posture
- Stronger internal controls for confidentiality, integrity, and availability
- Reduced risk of regulatory fines and reputational damage
- Standardized audit procedures across systems and teams
- Readiness for third-party audits and certifications

Instructional Methodology

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

- Strategy Briefings – Risk-based audit planning, frameworks, and key concepts
- Case Studies – Real-world breaches, audit failures, and regulatory actions
- Workshops – Audit checklists, gap analysis, and access reviews
- Peer Exchange – Sharing cross-industry audit experiences
- Tools – Sample audit plans, evidence logs, compliance matrices, and reporting templates

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

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: Information Security Audit Fundamentals

- Module 1: The Role of Information Security Audits (07:30 – 09:30) • Purpose, scope, and audit lifecycle • Risk-based approach and audit principles
- Module 2: Overview of ISMS Standards and Frameworks (09:45 – 11:15) • ISO/IEC 27001, NIST CSF, COBIT, GDPR • Clauses and controls relevant to auditing
- Module 3: Audit Planning and Risk Assessment (11:30 – 01:00) • Defining scope and objectives • Threat modeling and control mapping
- Module 4: Workshop – Develop an Audit Plan (02:00 – 03:30) • Build an audit scope and risk register for a case study

Day 2: Technical and Administrative Controls Review

- Module 1: Access Control and Identity Management (07:30 – 09:30) • User provisioning, segregation of duties, and role-based access • Password policies and MFA effectiveness
- Module 2: Network and System Security (09:45 – 11:15) • Firewall and endpoint protection auditing • Logs, alerts, and SIEM integration
- Module 3: Physical and Environmental Security (11:30 – 01:00) • Data center controls and physical access review • Visitor logs, CCTV, and disaster preparedness
- Module 4: Simulation – Access Review Audit (02:00 – 03:30) • Conduct sample access and privilege analysis

Day 3: Operational Security and Incident Preparedness

- Module 1: Change Management and System Hardening (07:30 – 09:30) • Patch management and secure configuration • Documentation and approval tracking
- Module 2: Backup, Recovery, and Business Continuity (09:45 – 11:15) • Data backup procedures and offsite storage audits • BCP/DRP compliance and test results
- Module 3: Incident Management and Breach Handling (11:30 – 01:00) • Incident response policies and logs • Case analysis: breaches and audit failures
- Module 4: Workshop – Audit of BCP/IR Controls (02:00 – 03:30) • Evaluate sample plans and test reports

Day 4: Compliance, Privacy, and Evidence Collection

- Module 1: Regulatory and Legal Compliance Audits (07:30 – 09:30) • GDPR, HIPAA, SOX, and cross-border data audits • Mapping legal obligations to ISMS controls
- Module 2: Data Classification and Retention (09:45 – 11:15) • Personal data handling, encryption, and retention policy review
- Module 3: Collecting and Validating Audit Evidence (11:30 – 01:00) • Interviewing, observation, and sampling • Evidence logs and traceability
- Module 4: Workshop – Conduct a Compliance Gap Analysis (02:00 – 03:30) • Map findings to audit objectives and recommend actions

Day 5: Audit Reporting and Continuous Improvement

- Module 1: Writing Audit Reports and Communicating Results (07:30 – 09:30) • Audit report format, clarity, and tone • Recommendations and risk ranking
- Module 2: Follow-up, Corrective Actions, and Re-audits (09:45 – 11:15) • Action tracking and management buy-in • CAPAs and lessons learned
- Module 3: Building a Long-Term Audit Program (11:30 – 01:00) • Annual planning, integration with enterprise risk • Automation tools and auditor skill development
-

Module 4: Final Presentation and Certification (02:00 – 03:30) • Group presentation of audit findings • Certification ceremony and feedback

Certification

Participants will receive a Certificate of Completion in Effective Information Security Audit, validating their proficiency in assessing information security frameworks, detecting control weaknesses, and supporting compliance with global cybersecurity 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**