

EFFECTIVE INFORMATION TECHNOLOGY (IT) AUDIT

“Auditing IT Systems, Processes, and Controls to Ensure Compliance, Security, and Operational Resilience”

Schedule

Date	Venue	Fees (Face-to-Face)
11 - 15 May 2026	London, UK	USD 3495 per delegate

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

Introduction

As organizations become increasingly dependent on digital infrastructure, IT audits play a critical role in verifying system integrity, cybersecurity, compliance, and risk management. A well-executed IT audit ensures that technology assets are protected, data is secure, and IT operations support business goals.

This intensive 5-day course provides auditors, IT professionals, and compliance teams with the knowledge and tools to assess IT governance, evaluate controls, identify vulnerabilities, and ensure regulatory compliance. Participants will be introduced to frameworks such as COBIT, NIST, ISO 27001, and ITIL, and will practice audit planning, execution, and reporting in an IT environment.

Objectives

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

- Plan and perform IT audits in alignment with business and regulatory requirements
- Evaluate IT governance, risk management, and control frameworks
- Assess security controls for networks, databases, applications, and cloud systems
- Identify vulnerabilities and audit findings with appropriate remediation actions
- Report on IT audit results clearly and effectively to both technical and non-technical stakeholders

Why Attend

- Build hands-on experience in auditing IT environments and technologies
- Learn to align IT audit procedures with international frameworks (COBIT, NIST, ISO 27001)
- Detect weaknesses in cybersecurity, system access, and data protection
- Develop audit programs for networks, data centers, and IT operations
- Enhance compliance with GDPR, SOX, HIPAA, and other IT-related regulations

Target Audience

This program is designed for:

- Internal and external auditors involved in IT systems
- IT managers, security officers, and risk professionals
- Governance, risk, and compliance (GRC) specialists
- Cybersecurity and information assurance professionals
- Anyone responsible for IT audit, monitoring, or assurance activities

Individual Benefits

Key competencies that will be developed include:

- IT audit planning, execution, and documentation
- Assessment of general and application controls
- Understanding of cybersecurity threats and mitigation
- Knowledge of IT governance and risk management frameworks
- Report writing and communication of audit findings

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved IT control effectiveness and security posture
- Reduced risk of cyber incidents and data breaches
- Enhanced regulatory compliance and audit readiness
- Stronger alignment between IT functions and business goals
- Consistency in IT auditing across systems and departments

Instructional Methodology

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

- Strategy Briefings - Key IT audit concepts, frameworks, and global standards
- Case Studies - IT failure incidents, cybersecurity audits, system breaches
- Workshops - Risk assessment, audit planning, vulnerability evaluation
- Peer Exchange - Audit scenarios and tool sharing across sectors
- Tools - IT audit checklists, risk registers, control matrices, NIST templates

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: IT Audit Foundations and Frameworks

- Module 1: Introduction to IT Auditing (07:30 - 09:30) • Scope, objectives, and types of IT audits
- Module 2: Governance and Control Frameworks (09:45 - 11:15) • COBIT, ISO 27001, ITIL, NIST overview
- Module 3: IT Risk Assessment Methodologies (11:30 - 01:00) • Threat identification, risk appetite, heat maps
- Module 4: Workshop - Map an IT Risk Register (02:00 - 03:30) • Identify and prioritize IT risks for an enterprise

Day 2: IT General Controls and Infrastructure

- Module 5: Assessing IT General Controls (07:30 - 09:30) • Change management, backup, recovery, logical access
- Module 6: Auditing Data Centers and IT Assets (09:45 - 11:15) • Physical security, environmental controls, asset tracking
- Module 7: IT Operations and Incident Management (11:30 - 01:00) • Monitoring tools, SLAs, helpdesk and ticketing reviews
- Module 8: Workshop - Develop a General Controls Checklist (02:00 - 03:30) • Design audit procedures for core IT services

Day 3: Application and Cybersecurity Controls

- Module 9: Application Control Auditing (07:30 - 09:30) • Input, processing, and output validation techniques
- Module 10: Cybersecurity Threats and Mitigation (09:45 - 11:15) • Firewall, antivirus, intrusion detection, patching
- Module 11: User Access Management (11:30 - 01:00) • Segregation of duties, privilege escalation, authentication
- Module 12: Workshop - Evaluate Cybersecurity Controls (02:00 - 03:30) • Conduct a gap analysis on a sample IT environment

Day 4: Cloud, Emerging Tech & Data Protection

- Module 13: Cloud Auditing Principles (07:30 - 09:30) • SaaS, IaaS, PaaS risks, shared responsibility model
- Module 14: Auditing Emerging Technologies (09:45 - 11:15) • AI, IoT, blockchain risks and control frameworks
- Module 15: Data Privacy and Regulatory Compliance (11:30 - 01:00) • GDPR, HIPAA, SOX IT requirements
- Module 16: Workshop - Audit a Cloud Implementation (02:00 - 03:30) • Assess vendor contracts, access, and data handling

Day 5: Reporting, Follow-Up, and Integration

- Module 17: IT Audit Reporting Best Practices (07:30 - 09:30) • Report structure, executive summaries, risk ranking
- Module 18: Corrective Actions and Follow-Up (09:45 - 11:15) • Action plans, root cause analysis, validation testing
- Module 19: Aligning IT Audit with Enterprise Strategy (11:30 - 01:00) • Bridging technical findings with business impact
- Module 20: Final Workshop - Simulate an End-to-End IT Audit (02:00 - 03:30) • Deliver a mock IT audit from planning to reporting

Certification

Participants will receive a Certificate of Completion in Effective Information Technology (IT) Audit, validating their ability to conduct structured, compliant, and risk-focused IT audits that enhance cyber resilience, data protection, and IT governance.

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.