MAWA EVENTS

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

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

IT RISK MANAGEMENT AUDIT: ASSESSES THE ORGANIZATION\'S PROCESSES FOR IDENTIFYING AND MANAGING IT-RELATED RISKS

“Auditing IT Risks to Strengthen Governance, Cybersecurity, and Operational Resilience”

Schedule

Date	Venue	Fees (Face-to-Face)
09 – 13 Nov 2026	London – UK	USD 3495 per delegate

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

Introduction

In the digital age, managing IT risk is essential for ensuring business continuity, protecting data, and complying with regulatory requirements. Organizations must identify, evaluate, and mitigate risks related to IT infrastructure, applications, cybersecurity, and third-party service providers.

This intensive training program equips auditors, IT risk professionals, and compliance teams with the tools and frameworks to assess IT risk management practices effectively. Participants will learn how to audit IT governance, controls, and risk responses in alignment with global standards such as COBIT, ISO 27005, and NIST.

Objectives

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

- Identify, evaluate, and prioritize IT risks across systems and processes
- Conduct IT risk audits using a structured, risk-based approach
- Assess the effectiveness of IT governance and control frameworks
- Evaluate cybersecurity and third-party risk management practices
- Provide assurance and recommendations aligned with best practices and standards

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

- Strengthen your audit approach to rapidly evolving IT risks
- Learn global IT risk frameworks and how to apply them in audit engagements
- Support organizational resilience through improved risk mitigation strategies
- Bridge the gap between technical controls and business risk management
- Enhance IT audit effectiveness in areas like cybersecurity, cloud, and data privacy

Target Audience

This program is designed for:

- Internal and IT auditors
- IT risk and compliance officers
- Information security professionals
- Governance, risk, and control (GRC) specialists
- Managers responsible for IT strategy, operations, or oversight

Individual Benefits

Key competencies that will be developed include:

- IT risk assessment techniques and reporting
- Understanding of IT governance frameworks (e.g., COBIT, ISO, NIST)
- Evaluation of technical and process-level controls
- Cyber risk auditing and third-party risk management
- Skills to communicate findings to both technical and executive stakeholders

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved identification and mitigation of technology-related risks
- Better integration of IT audit with enterprise risk management (ERM)
- Enhanced ability to assure IT resilience, compliance, and data integrity
- Reduced exposure to cyber threats and system vulnerabilities
- Stronger IT governance and strategic alignment

Instructional Methodology

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

- Strategy Briefings – IT risk management frameworks, audit standards, and governance models
- Case Studies – High-profile IT risk failures and audit investigations
- Workshops – Risk assessments, control evaluations, and audit planning exercises
- Peer Exchange – Shared experiences in IT risk auditing across sectors
- Tools – IT risk audit checklists, scoring matrices, and reporting templates

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: IT Risk Landscape and Audit Fundamentals

- Module 1: Understanding IT Risk Domains (07:30 – 09:30) • Types of IT risks: operational, strategic, compliance, and cybersecurity • Key IT risk sources: systems, processes, third parties, and users
- Module 2: IT Risk Management Frameworks (09:45 – 11:15) • Overview of ISO 27005, COBIT 2019, and NIST RMF • ERM and IT risk integration
- Module 3: Workshop – Building an IT Risk Register (11:30 – 01:00) • Identify and categorize risks for a sample organization
- Module 4: Peer Exchange – IT Risk Prioritization Challenges (02:00 – 03:30) • Group discussion on risk tolerance and risk appetite

Day 2: Risk-Based IT Audit Planning

- Module 5: Audit Planning and Scoping for IT Risk (07:30 – 09:30) • Defining audit objectives, criteria, and engagement scope • Mapping IT assets and risk exposures
- Module 6: Control Frameworks and Audit Standards (09:45 – 11:15) • ITGCs, application controls, and cybersecurity controls • Using COBIT and NIST in audit execution
- Module 7: Workshop – Risk-Based IT Audit Plan (11:30 – 01:00) • Design an audit program for an IT risk scenario
- Module 8: Case Study – Audit Failure and Oversight (02:00 – 03:30) • Lessons learned from a high-profile IT breakdown

Day 3: Cybersecurity and Technical Control Evaluation

- Module 9: Auditing Cybersecurity Risk Management (07:30 – 09:30) • Controls for access, network security, malware, and incident response • Reviewing security operations and monitoring tools
- Module 10: Cloud, Remote Access, and Emerging Risks (09:45 – 11:15) • Risks in SaaS, IaaS, BYOD, and hybrid environments • Cloud security posture management
- Module 11: Workshop – Evaluating Cybersecurity Controls (11:30 – 01:00) • Score cybersecurity control effectiveness and identify gaps
- Module 12: Peer Exchange – Cyber Risk and Audit Alignment (02:00 – 03:30) • Sharing strategies to audit fast-changing threat landscapes

Day 4: Third-Party Risk and Incident Auditing

- Module 13: Auditing Third-Party and Vendor Risks (07:30 – 09:30) • Due diligence, SLAs, and contract compliance • Risk transfer and monitoring
- Module 14: Incident Management and Response Auditing (09:45 – 11:15) • Assessing IR plans, breach response, and forensic readiness • Lessons from real-world cyberattacks
- Module 15: Workshop – Simulated Incident Audit (11:30 – 01:00) • Audit a mock data breach response
- Module 16: Group Discussion – Vendor Risk and Shared Accountability (02:00 – 03:30) • Peer feedback on third-party governance practices

Day 5: Reporting, Follow-Up, and Audit Effectiveness

Module 17: Audit Findings and Risk Communication (07:30 – 09:30) • Crafting impactful audit reports with actionable recommendations • Linking technical issues to business impact

Module 18: Tracking Remediation and Audit Follow-Up (09:45 – 11:15) • Remediation ownership, timelines, and verification

Module 19: Final Project – IT Risk Audit Presentation (11:30 – 01:00) • Present audit results for a risk-based case scenario

Module 20: Wrap-Up, Feedback, and Certification (02:00 – 03:30) • Course review, discussion, and certificate awarding

MAWA EVENTS

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

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

Certification

Participants will receive a Certificate of Completion in IT Risk Management Audit, validating their ability to assess, report, and support the mitigation of IT-related risks using global best practices and frameworks.

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**