MAWA EVENTS

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

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

CYBERSECURITY AUDIT: ASSESSES THE OVERALL CYBERSECURITY POSTURE OF AN ORGANIZATION, INCLUDING POLICIES, PROCESSES, AND TECHNICAL CONTROLS

“Evaluate and Strengthen Your Organization\'s Cybersecurity with Expert-Led Audits”

Schedule

Date	Venue	Fees (Face-to-Face)
06– 10 Jul 2026	London, UK	USD 4995 per delegate

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

Introduction

This five-day course is designed to provide professionals with the necessary tools and techniques to conduct a comprehensive cybersecurity audit. It covers the assessment of an organization\'s cybersecurity posture, focusing on policies, processes, and technical controls. Participants will learn how to evaluate cybersecurity risks, identify vulnerabilities, and assess the overall security readiness of an organization.

The training combines theoretical learning with practical exercises, case studies, and peer exchange to ensure participants gain hands-on experience in auditing cybersecurity practices. The goal is to equip delegates with the skills to perform thorough cybersecurity audits, strengthen security frameworks, and ensure compliance with global cybersecurity standards.

Objectives

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

- Understand the key principles and processes of cybersecurity auditing
- Assess an organization’s cybersecurity posture, including policies, processes, and technical controls
- Identify common vulnerabilities and risks within an organization’s cybersecurity framework
- Develop actionable recommendations for improving security measures
- Conduct comprehensive audits and prepare detailed audit reports

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 organization’s cybersecurity by identifying critical vulnerabilities
- Gain in-depth knowledge of cybersecurity auditing principles and practices
- Learn from experts with real-world experience in cybersecurity audits
- Access templates, tools, and methodologies for immediate use

Target Audience

This program is designed for:

- IT auditors and cybersecurity professionals
- Risk management and compliance officers
- Information security officers (CISOs)
- Security analysts and consultants responsible for cybersecurity assessments
- Professionals involved in assessing and improving organizational security posture

Individual Benefits

Key competencies that will be developed include:

- Enhanced expertise in cybersecurity auditing and risk assessment
- Advanced skills in identifying cybersecurity vulnerabilities and gaps
- Proficiency in conducting cybersecurity audits using industry best practices
- Knowledge of tools and techniques for assessing and improving cybersecurity frameworks
- Ability to provide actionable recommendations for improving cybersecurity measures

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- A comprehensive understanding of cybersecurity risks and how to mitigate them
- Improved ability to evaluate and strengthen organizational cybersecurity measures
- Stronger alignment of cybersecurity practices with regulatory requirements and industry standards
- Enhanced ability to identify and address vulnerabilities before they lead to security breaches
- A more proactive and resilient cybersecurity posture across the organization

Instructional Methodology

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

- Strategy Briefings – Detailed overview of cybersecurity auditing principles and methodologies
- Case Studies – Real-world examples of cybersecurity breaches and audit findings
- Workshops – Hands-on exercises to assess cybersecurity frameworks and identify risks
- Peer Exchange – Group discussions on common challenges and lessons learned in cybersecurity auditing
- Tools – Templates and checklists for conducting audits and preparing security reports

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: Introduction to Cybersecurity Audits and Frameworks

- Module 1: Overview of Cybersecurity Auditing (07:30 – 09:30)
- Defining cybersecurity auditing and its importance in risk management
- Key principles and processes of cybersecurity audits
- Overview of common audit frameworks and standards (e.g., NIST, ISO/IEC 27001)
- Module 2: Cybersecurity Risk Assessment (09:45 – 11:15)
- Understanding the threat landscape and identifying organizational risks
- Risk assessment methodologies and techniques
- Tools for identifying vulnerabilities and threats
- Module 3: The Role of Policies and Procedures (11:30 – 01:00)
- Importance of cybersecurity policies and procedures in an audit
- How to evaluate and audit policies for effectiveness
- Ensuring compliance with cybersecurity regulations and standards

Day 2: Auditing Technical Controls and Infrastructure

- Module 4: Auditing Technical Controls (07:30 – 09:30)
- Assessing network security controls (firewalls, intrusion detection systems)
- Evaluating endpoint security and data protection measures
- Auditing access control systems and authentication mechanisms
- Module 5: Vulnerability Assessment Tools (09:45 – 11:15)
- Introduction to vulnerability scanning tools and techniques
- How to use vulnerability management tools to identify weaknesses
- Best practices for remediating vulnerabilities
- Module 6: Audit of Incident Response and Recovery Plans (11:30 – 01:00)
- Evaluating incident response and disaster recovery plans
- Ensuring preparedness for potential cyber incidents
- Auditing the effectiveness of crisis communication strategies

Day 3: Conducting the Cybersecurity Audit

- Module 7: Preparing for a Cybersecurity Audit (07:30 – 09:30)
- Defining the scope and objectives of the cybersecurity audit
- Planning and scheduling the audit process
- Key stakeholders and resources needed for a successful audit
- Module 8: Data Collection and Audit Execution (09:45 – 11:15)
- Techniques for gathering data during the audit process
- Conducting interviews and document reviews
- Using audit tools to assess security practices
- Module 9: Identifying Key Findings (11:30 – 01:00)
- How to identify critical cybersecurity weaknesses during the audit
- Prioritizing findings based on risk and impact
-

Preparing for the final audit report

Day 4: Reporting and Recommendations

- Module 10: Writing the Cybersecurity Audit Report (07:30 – 09:30)
- Structuring the audit report for clarity and impact
- Best practices for reporting findings and recommendations
- How to present audit results to senior management
- Module 11: Creating Actionable Recommendations (09:45 – 11:15)
- Developing practical recommendations to mitigate cybersecurity risks
- Aligning recommendations with organizational goals and resources
- Best practices for implementing cybersecurity improvements
- Module 12: Audit Follow-Up and Continuous Improvement (11:30 – 01:00)
- How to track and follow up on audit findings and recommendations
- Continuous improvement in cybersecurity practices
- Monitoring the effectiveness of cybersecurity controls over time

Day 5: Advanced Cybersecurity Auditing Techniques and Future Trends

- Module 13: Advanced Techniques in Cybersecurity Auditing (07:30 – 09:30)
- Conducting audits of emerging technologies (cloud security, IoT, AI)
- Audit techniques for assessing advanced cybersecurity measures
- Addressing new and evolving threats in the cybersecurity landscape
- Module 14: Cybersecurity Auditing in a Global Context (09:45 – 11:15)
- Understanding the international cybersecurity landscape
- Global standards and regulations in cybersecurity auditing
- How to audit for compliance with global cybersecurity laws
- Module 15: Final Review and Wrap-Up (11:30 – 01:00)
- Case study and group discussion on lessons learned
- Final Q&A and course review
- Closing remarks and certification

Certification

Participants will receive a Certificate of Completion in Cybersecurity Audit, validating their expertise in assessing and auditing cybersecurity frameworks, practices, and controls.

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**