MAWA EVENTS

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

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

NETWORK SECURITY AUDIT: FOCUSES ON ASSESSING THE SECURITY OF AN ORGANIZATION\'S NETWORK INFRASTRUCTURE

""Assessing and Strengthening the Security of Your Organization's Network Infrastructure""

Schedule

Date	Venue	Fees (Face-to-Face)
16 – 20 Mar 2026	London, UK	USD 3495 per delegate

Introduction

With rising cyber threats, increasing regulatory demands, and growing reliance on interconnected systems, securing the network infrastructure has become a critical business priority. Internal audit and IT security teams must be equipped to assess network defenses, detect vulnerabilities, and evaluate the effectiveness of security controls.

This 5-day course provides a structured framework for auditing network security across both on-premises and cloud environments. Participants will explore risk-based audit planning, review firewall configurations, assess access and monitoring controls, and understand how to evaluate network architecture against best practices and standards like ISO 27001, NIST, and CIS Controls.

Objectives

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

- Understand the principles of network architecture, components, and protocols
- Evaluate security controls across firewalls, routers, switches, and wireless systems
- Identify network vulnerabilities and assess threat exposure
- Design and execute network security audits using recognized frameworks
- Report audit findings and recommend technical and governance improvements

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

- Gain a deep understanding of network environments from an auditor’s perspective
- Learn how to evaluate internal and perimeter defenses for effectiveness
- Apply proven methodologies to test access controls, intrusion detection, and logging
- Support regulatory and cybersecurity compliance through structured audits
- Improve your organization’s resilience against cyberattacks and data breaches

Target Audience

This program is designed for:

- IT auditors and internal auditors
- Cybersecurity and network security professionals
- Risk and compliance officers
- Network engineers and administrators involved in security assurance
- Anyone responsible for assessing or improving network security controls

Individual Benefits

Key competencies that will be developed include:

- Network architecture understanding from a risk/audit lens
- Firewall and perimeter security audit techniques
- Intrusion detection and vulnerability management review
- Wireless and remote access control evaluation
- Technical reporting of network security risks

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Strengthened defenses against external and internal cyber threats
- Better visibility into network security weaknesses and gaps
- Improved compliance with ISO 27001, NIST, CIS, and internal policies
- Clearer audit reporting for stakeholders and board oversight
- Integration of network security into broader IT governance and assurance programs

Instructional Methodology

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

- Strategy Briefings – Network security principles, controls, and risk areas
- Case Studies – Real-world network breaches and audit failures
- Workshops – Firewall rule reviews, vulnerability scans, and log audits
- Peer Exchange – Audit challenges and success stories from participants
- Tools – Audit checklists, risk scoring templates, and test plans

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

Training Hours: 07:30 AM – 03:30 PM Daily Format: 3–4 Learning Modules | Coffee Breaks: 09:30 & 11:15 | Lunch Break: 01:00 – 02:00

Day 1: Understanding Network Environments and Risks

- Module 1: Network Architecture and Protocols (07:30 – 09:30) • Components: routers, switches, firewalls, IDS/IPS • TCP/IP, VLANs, DNS, DHCP, and tunneling protocols • Common attack vectors in modern networks
- Module 2: Threats and Vulnerabilities (09:45 – 11:15) • Internal vs external threats • Network attack techniques: spoofing, sniffing, DoS/DDoS • Asset classification and exposure rating
- Module 3: Workshop – Network Risk Mapping (11:30 – 01:00) • Identify critical network assets and threat sources

Day 2: Access Control and Perimeter Defense

- Module 4: Firewalls and Edge Device Security (07:30 – 09:30) • Firewall types and configuration review • NAT, ACLs, and rulebase evaluation • Firewall log analysis
- Module 5: Remote Access and VPN Controls (09:45 – 11:15) • VPN types and secure tunneling • Remote access risks and controls • MFA, encryption, and endpoint security
- Module 6: Workshop – Firewall Configuration Review (11:30 – 01:00) • Audit simulation of firewall and VPN setup

Day 3: Monitoring, Intrusion Detection, and Wireless Audit

- Module 7: Logging and Network Monitoring (07:30 – 09:30) • Syslog, SIEM, and log correlation tools • Log retention policies and red flag events • Testing logging completeness
- Module 8: IDS/IPS and Threat Detection (09:45 – 11:15) • Placement and configuration of IDS/IPS systems • Signature vs anomaly detection • Alert tuning and escalation procedures
- Module 9: Wireless Network Security (11:30 – 01:00) • Common wireless threats (WEP crack, rogue APs) • WPA3, MAC filtering, SSID cloaking • Auditing wireless coverage and segmentation

Day 4: Audit Planning and Testing Techniques

- Module 10: Network Security Audit Planning (07:30 – 09:30) • Scoping audits across on-prem and cloud infrastructure • Sampling techniques and walkthroughs • Asset inventories and topology mapping
- Module 11: Audit Testing and Evidence Gathering (09:45 – 11:15) • Testing firewall rules, VLAN configurations, access lists • Use of scanning tools (Nmap, Nessus, Wireshark) • Documentation and screenshots for audit evidence
- Module 12: Workshop – Performing a Sample Network Audit (11:30 – 01:00) • Participants conduct a simulated audit of a sample network

Day 5: Reporting, Compliance, and Governance Alignment

- Module 13: Regulatory and Framework Alignment (07:30 – 09:30) • ISO 27001, NIST CSF, CIS Controls, and local laws • Linking network audits to cybersecurity strategy
- Module 14: Audit Reporting and Communication (09:45 – 11:15) • Writing clear and risk-prioritized audit findings • Recommendations for technical and procedural remediation
- Module 15: Final Simulation – Audit Report Presentation (11:30 – 01:00) • Participants present audit findings and defend conclusions

Certification

Participants will receive a Certificate of Completion in Network Security Audit, validating their ability to assess, test, and report on the security of an organization’s network infrastructure in alignment with global cybersecurity 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 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**