MAWA EVENTS

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

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

REMOTE ACCESS SECURITY AUDIT: EVALUATES THE SECURITY CONTROLS FOR REMOTE ACCESS TO ORGANIZATIONAL SYSTEMS

"Securing Remote Connectivity through Rigorous Audit and Control Frameworks"

Schedule

Date	Venue	Fees (Face-to-Face)
25 – 29 May 2026	London, UK	USD 3495 per delegate

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

Introduction

As organizations embrace hybrid work models, cloud services, and third-party collaborations, secure remote access has become a cornerstone of IT operations. However, remote connectivity also expands the attack surface and introduces new risks such as credential theft, unauthorized access, data leakage, and malware propagation.

This intensive 5-day training enables IT auditors, cybersecurity professionals, and risk managers to assess and strengthen the security of remote access systems. Participants will explore VPNs, virtual desktops, secure gateways, Zero Trust architectures, and identity controls, while using global frameworks such as NIST SP 800-46, ISO/IEC 27033, and CIS benchmarks to guide effective audit and reporting.

Objectives

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

- Identify and audit all remote access mechanisms (VPNs, RDP, SSH, VDI, cloud)
- Evaluate identity and access management (IAM), authentication, and endpoint controls
- Assess the effectiveness of monitoring, logging, and incident response for remote sessions
- Map risks to control gaps and compliance obligations
- Generate audit findings and prioritize corrective actions for enhanced security posture

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

- Ensure secure access to critical systems from remote locations
- Strengthen audit capacity over BYOD, third-party, and mobile access channels
- Apply leading audit frameworks for remote access technologies
- Uncover vulnerabilities in remote desktop, VPN, cloud, and identity infrastructures
- Support Zero Trust, ISO 2

Target Audience

This program is designed for:

- IT and cybersecurity auditors
- Network and security engineers
- IT compliance officers and risk managers
- Remote infrastructure administrators
- Anyone responsible for access governance and cybersecurity assurance7001, NIST, and organizational cybersecurity goals

Individual Benefits

Key competencies that will be developed include:

- Remote access control assessment and technical audit execution
- Vulnerability detection across remote channels
- Log review and evidence gathering for remote activity
- Authentication, encryption, and endpoint audit techniques
- Reporting and remediation planning aligned with risk exposure

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Reduced remote access vulnerabilities and threat exposure
- Improved regulatory and policy compliance across access channels
- More secure hybrid and mobile work environments
- Evidence-based remote access audit processes and risk reporting
- Stronger alignment with cybersecurity frameworks and IT governance

Instructional Methodology

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

- Standards Briefings – NIST, ISO/IEC 27033, CIS Benchmarks, and Zero Trust
- Real-World Cases – Remote access breaches and audit findings
- Audit Simulations – VPN, remote desktop, cloud access audit walkthroughs
- Hands-On Workshops – Checklist design, risk mapping, and control evaluation
- Tools & Templates – Audit logs, policy checklists, scoring matrices

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: 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: Remote Access Landscape and Audit Fundamentals

- Module 1: Understanding Remote Access Architectures (07:30 – 09:30) • VPN, RDP, VDI, SSH, and cloud-based access • Use cases and associated risks
- Module 2: Audit Standards and Policy Frameworks (09:45 – 11:15) • NIST SP 800-46, ISO/IEC 27033, CIS controls • Remote access policy elements
- Module 3: Remote Access Threats and Risk Scenarios (11:30 – 01:00) • Compromised credentials, rogue devices, lateral movement • Insider threat and access abuse
- Module 4: Workshop – Define a Remote Access Audit Scope (02:00 – 03:30) • Map systems, stakeholders, and threats in a sample audit plan

Day 2: Authentication, Encryption, and Access Control

- Module 5: Authentication Methods and MFA (07:30 – 09:30) • Passwords, OTP, biometrics, hardware tokens • Multi-factor authentication design and audit points
- Module 6: Remote Access Encryption and Tunneling (09:45 – 11:15) • SSL/TLS, IPSec, SSH • VPN configuration and tunnel validation
- Module 7: Role-Based Access and IAM Controls (11:30 – 01:00) • Directory services, RBAC/ABAC • Least privilege enforcement
- Module 8: Workshop – Audit User Access for a Remote Work Group (02:00 – 03:30) • Review role assignments and identify privilege creep

Day 3: Device Security, Logging, and Monitoring

- Module 9: Endpoint Controls and Device Hardening (07:30 – 09:30) • Antivirus, firewalls, patching, remote wipe • BYOD and managed vs unmanaged device controls
- Module 10: Log Management and Audit Trails (09:45 – 11:15) • What to log and how to analyze access events • Log retention and SIEM integration
- Module 11: Monitoring Remote Activity and Anomalies (11:30 – 01:00) • Indicators of compromise (IOC) and behavioral analytics • Alerting and escalation mechanisms
- Module 12: Workshop – Review Remote Session Logs (02:00 – 03:30) • Identify risky patterns and unusual access events

Day 4: Compliance, Testing, and Incident Response

- Module 13: Regulatory and Framework Alignment (07:30 – 09:30) • GDPR, HIPAA, PCI DSS remote access clauses • Alignment with ISO/IEC 27001 audits
- Module 14: Remote Access Testing and Vulnerability Scanning (09:45 – 11:15) • Pen-testing VPNs and RDP exposure • Port scans, brute-force detection, exploit checks
- Module 15: Incident Detection and Response (11:30 – 01:00) • Playbooks for compromised remote access • Coordination with SOC and IT teams
- Module 16: Workshop – Conduct a Remote Access Risk Assessment (02:00 – 03:30) • Use risk heat maps and scoring for prioritization

Day 5: Strategic Reporting and Final Audit Simulation

- Module 17: Reporting Audit Findings and Recommendations (07:30 – 09:30) • Structure, clarity, risk language, visuals • Actionable vs advisory recommendations
- Module 18: Remediation Planning and Risk Mitigation (09:45 – 11:15) • Controls improvement strategies • Short- vs long-term actions
- Module 19: Capstone Simulation – Full Remote Access Audit (11:30 – 01:00) • Group presentation on remote access audit case
- Module 20: Course Debrief and Certificate Ceremony (02:00 – 03:30) • Feedback, learning review, certificate distribution

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 Remote Access Security Audit, validating their ability to assess, test, and report on remote access security controls in alignment with international frameworks, risk-based methodologies, and industry best practices.

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**