MAWA EVENTS

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

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

IOT SECURITY AUDIT: ASSESSES THE SECURITY CONTROLS FOR INTERNET OF THINGS (IOT) DEVICES AND SYSTEMS

"Mitigating Cyber Risks in IoT Infrastructures through Effective Security Auditing"

Schedule

Date	Venue	Fees (Face-to-Face)
12 – 16 Oct 2026	London, UK	USD 3495 per delegate

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

Introduction

As the number of connected devices continues to grow, organizations face unprecedented risks to their networks, data, and operations through the Internet of Things (IoT). From smart sensors and industrial controllers to wearables and connected appliances, IoT systems often lack sufficient security by design, making them prime targets for cyberattacks.

This intensive course provides professionals with the practical skills and methodologies to plan and perform comprehensive IoT security audits. Participants will learn how to assess the entire IoT ecosystem—including devices, networks, applications, and cloud services—to identify vulnerabilities, evaluate control effectiveness, and ensure compliance with emerging IoT cybersecurity standards.

Objectives

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

- Understand IoT architectures, protocols, and attack surfaces
- Conduct structured audits of IoT devices, data flows, and management platforms
- Evaluate the security of embedded systems, firmware, and device communication
- Assess network segmentation, access controls, and monitoring for IoT environments
- Report vulnerabilities and control gaps in line with NIST, ENISA, and ISO 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

- Protect your organization from IoT-related cyber threats and data breaches
- Assess security postures across consumer, industrial, and enterprise IoT systems
- Apply risk-based auditing to devices, cloud services, and third-party platforms
- Strengthen compliance with privacy laws and security regulations
- Enhance your audit team’s readiness for the evolving IoT threat landscape

Target Audience

This program is designed for:

- IT auditors and cybersecurity professionals
- IoT architects, network and systems engineers
- Risk, compliance, and assurance officers
- OT security specialists in manufacturing, utilities, and healthcare
- Anyone responsible for securing or evaluating connected devices and infrastructure

Individual Benefits

Key competencies that will be developed include:

- IoT risk identification and threat modeling
- Assessment of device-level and network-level security
- Knowledge of IoT protocols and audit frameworks (MQTT, CoAP, Zigbee, etc.)
- Vulnerability scanning and firmware audit techniques
- IoT-specific reporting and remediation planning

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved IoT asset visibility and risk posture
- Enhanced protection of industrial and smart technologies
- Reduced risk of operational disruption or data compromise
- Compliance with cybersecurity mandates and supply chain controls
- A proactive approach to secure-by-design device environments

Instructional Methodology

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

- Strategy Briefings – IoT security frameworks, risks, and audit challenges
- Case Studies – Breaches and audit findings across industrial and consumer sectors
- Workshops – IoT threat modeling, audit plan development, and control testing
- Peer Exchange – Sector-specific insights and mitigation strategies
- Tools – Audit templates, asset inventory models, protocol analyzers, and reporting guides

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 IoT Ecosystems and Risks

- Module 1: IoT Fundamentals and Audit Scope (07:30 – 09:30) • IoT use cases, technologies, and architecture layers • Defining audit scope for complex IoT environments
- Module 2: IoT Threat Landscape and Attack Vectors (09:45 – 11:15) • Common vulnerabilities: insecure interfaces, firmware flaws, hardcoded credentials
- Module 3: Global IoT Security Standards Overview (11:30 – 01:00) • NIST 8259, ETSI EN 303 645, OWASP Top 10 for IoT
- Module 4: Workshop – IoT Threat Modeling (02:00 – 03:30) • Map threats to a sample IoT architecture

Day 2: Auditing IoT Devices and Embedded Systems

- Module 1: Firmware and Embedded Software Security (07:30 – 09:30) • Code review, binary analysis, update mechanisms
- Module 2: Authentication and Access Control in IoT Devices (09:45 – 11:15) • Role-based access, credential management, secure boot
- Module 3: Device Hardening and Physical Security (11:30 – 01:00) • Ports, debugging interfaces, tamper-proofing
- Module 4: Workshop – Firmware Vulnerability Analysis (02:00 – 03:30) • Analyze a simulated IoT firmware image

Day 3: IoT Network and Communication Security

- Module 1: IoT Communication Protocols and Encryption (07:30 – 09:30) • MQTT, CoAP, Zigbee, BLE, LoRaWAN – audit implications
- Module 2: Network Segmentation and Monitoring (09:45 – 11:15) • Firewalls, IDS/IPS, micro-segmentation
- Module 3: Logging, Event Management, and Intrusion Detection (11:30 – 01:00) • Log configuration and security event review
- Module 4: Workshop – Network Security Audit for IoT Setup (02:00 – 03:30) • Design and assess an IoT network audit checklist

Day 4: Cloud Services, Privacy, and Third-Party Audits

- Module 1: IoT Cloud Architecture and API Security (07:30 – 09:30) • Authentication, data protection, API vulnerabilities
- Module 2: Privacy and Data Protection Compliance (09:45 – 11:15) • GDPR, CCPA, and IoT-specific data handling
- Module 3: Vendor Risk Management and Supply Chain Security (11:30 – 01:00) • Third-party controls and remote update validation
- Module 4: Workshop – Cloud Security and Data Privacy Gap Analysis (02:00 – 03:30) • Audit a cloud-based IoT platform

Day 5: Reporting, Remediation & Certification

- Module 1: IoT Audit Findings and Prioritization (07:30 – 09:30) • Severity scoring, risk heat maps, actionable recommendations
- Module 2: Audit Reporting and Follow-Up (09:45 – 11:15) • Communicating findings to IT, engineering, and leadership
- Module 3: Final Group Audit Simulation and Presentations (11:30 – 01:00) • Team exercise on an end-to-end IoT audit case
- Module 4: Certification & Wrap-Up (02:00 – 03:30) • Course review, implementation plans, and certificate distribution

Certification

Participants will receive a Certificate of Completion in IoT Security Audit, confirming their ability to assess, report, and enhance the security posture of connected devices, networks, and platforms across IoT environments.

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.

MAWA EVENTS

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

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

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: **+601116373203**	EMAIL: **info@mawaevents.net**