MAWA EVENTS

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

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

SMART DEVICE SECURITY AUDIT: EXAMINES THE SECURITY OF INTERNET OF THINGS (IOT) DEVICES USED WITHIN THE ORGANIZATION

“Protect Your Organization\'s IoT Devices and Networks from Emerging Security Threats”

Schedule

Date	Venue	Fees (Face-to-Face)
06– 10 Jul 2026	London, UK	USD 3495 per delegate

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

Introduction

The Smart Device Security Audit course is designed to provide participants with the knowledge and skills required to evaluate and secure Internet of Things (IoT) devices used in organizations. As IoT devices proliferate across industries, ensuring their security is critical to protecting sensitive data and maintaining network integrity. This course will focus on the unique vulnerabilities associated with IoT devices, strategies for securing them, and how to perform effective security audits.

Participants will learn how to identify security risks specific to IoT environments, including unsecured devices, network vulnerabilities, and data protection challenges. The course also covers compliance standards, security frameworks, and practical solutions for securing IoT devices and networks.

Objectives

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

- Assess the security posture of IoT devices and networks
- Identify vulnerabilities and risks associated with smart devices and IoT environments
- Implement effective security measures to secure IoT devices and communications
- Conduct comprehensive security audits of IoT devices, identifying gaps and weaknesses
- Develop a strategy for maintaining ongoing IoT security and ensuring compliance with relevant regulations

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

- Learn how to secure IoT devices from evolving cybersecurity threats
- Understand the unique security challenges posed by smart devices and IoT ecosystems
- Gain expertise in IoT security auditing, including risk assessment and vulnerability management
- Learn how to implement best practices for securing networks, devices, and data within IoT environments
- Develop a solid understanding of compliance requirements for IoT device security

Target Audience

This program is designed for:

- IT auditors and cybersecurity professionals
- IoT developers and engineers
- Network security managers
- Compliance officers and risk managers
- Anyone responsible for managing or auditing the security of smart devices or IoT systems in an organization

Individual Benefits

Key competencies that will be developed include:

- Expertise in IoT device security and vulnerability management
- Ability to perform IoT security audits and assessments
- Proficiency in securing communication networks used by smart devices
- Understanding of regulatory compliance requirements related to IoT security
- Skills in developing and implementing security protocols for IoT devices

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved ability to secure IoT devices and protect organizational data from cyber threats
- Enhanced capability to assess and mitigate IoT-specific security risks
- Knowledge of compliance frameworks and how to align IoT security with industry standards
- A proactive approach to managing IoT security and ensuring organizational resilience
- Increased understanding of how to implement effective security measures for a connected IoT infrastructure

Instructional Methodology

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

- Strategy Briefings – Introduction to IoT security risks, challenges, and solutions
- Case Studies – Examination of real-world IoT security breaches and successful defense strategies
- Workshops – Hands-on exercises for performing IoT security audits and risk assessments
- Peer Exchange – Group discussions on securing smart devices and overcoming IoT security challenges
- Tools – Security assessment frameworks, audit templates, and IoT security protocols

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 Smart Device Security and IoT Ecosystems

- Module 1: IoT Security Overview (07:30 – 09:30)
- Importance of securing IoT devices and networks
- Key vulnerabilities and threats in IoT ecosystems
- Regulatory and compliance requirements for IoT security
- Module 2: IoT Architecture and Security Frameworks (09:45 – 11:15)
- Overview of IoT architecture and components
- Security frameworks for IoT (e.g., NIST, ISO/IEC 27001)
- IoT device lifecycle and security management
- Module 3: Key IoT Security Threats (11:30 – 01:00)
- Common IoT security vulnerabilities (e.g., weak authentication, data interception)
- Real-world IoT security breaches and lessons learned
- Emerging threats to IoT environments

Day 2: Conducting IoT Security Audits

- Module 4: Preparing for an IoT Security Audit (07:30 – 09:30)
- Defining audit objectives and scope for IoT devices
- Gathering relevant data and tools for auditing IoT security
- Key areas to assess during an IoT security audit
- Module 5: Performing an IoT Security Assessment (09:45 – 11:15)
- Conducting risk assessments for IoT devices and networks
- Identifying vulnerabilities and assessing device security configurations
- Tools and techniques for IoT security testing and audit
- Module 6: IoT Communication Protocols and Network Security (11:30 – 01:00)
- Securing communication channels used by IoT devices
- Best practices for IoT network security (e.g., segmentation, firewalls)
- Assessing the security of cloud-based IoT platforms

Day 3: Securing IoT Devices and Networks

- Module 7: Securing IoT Devices (07:30 – 09:30)
- Device hardening techniques and firmware security
- Implementing strong authentication and access control measures
- Securing device storage and data protection methods
- Module 8: IoT Encryption and Privacy Considerations (09:45 – 11:15)
- Best practices for IoT encryption and data protection
- Managing privacy concerns with IoT devices
- IoT-specific privacy regulations (e.g., GDPR, CCPA)
- Module 9: Monitoring and Incident Response for IoT Devices (11:30 – 01:00)
- Continuous monitoring techniques for IoT environments
- Responding to security incidents involving IoT devices
-

Developing an incident response plan for IoT security breaches

Day 4: Managing IoT Security Risks

- Module 10: Risk Mitigation Strategies for IoT Security (07:30 – 09:30)
- Mitigating common IoT security risks (e.g., insecure devices, weak encryption)
- Best practices for IoT risk management and mitigation
- Implementing security patches and updates for IoT devices
- Module 11: Compliance and Regulatory Frameworks (09:45 – 11:15)
- Aligning IoT security practices with compliance standards (e.g., NIST, ISO 27001)
- Understanding regulatory requirements for IoT security
- Auditing IoT devices for compliance with industry regulations
- Module 12: Building a Robust IoT Security Strategy (11:30 – 01:00)
- Developing an organizational strategy for IoT security
- Integrating IoT security with broader cybersecurity policies
- Establishing a culture of security within IoT environments

Day 5: Final Assessment and Certification

- Module 13: Group Exercise: IoT Security Audit Simulation (07:30 – 09:30)
- Conducting a mock IoT security audit and identifying vulnerabilities
- Peer feedback and analysis of audit results
- Presenting audit findings and recommendations
- Module 14: Final Review and Q&A (09:45 – 11:15)
- Final review of key topics and best practices for IoT security
- Addressing any remaining questions and concerns
- Module 15: Certification and Closing Remarks (11:30 – 01:00)
- Distribution of certificates of completion
- Closing remarks and next steps for securing IoT devices

Certification

Participants will receive a Certificate of Completion in Smart Device Security Audit, validating their ability to assess and secure IoT devices, mitigate risks, and implement security measures to protect connected devices and networks.

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**