MAWA EVENTS

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

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

MOBILE SECURITY AUDIT: EXAMINES THE SECURITY OF MOBILE DEVICES AND APPLICATIONS USED WITHIN AN ORGANIZATION

"Protecting Enterprise Data and Infrastructure Across Mobile Platforms"

Schedule

Date	Venue	Fees (Face-to-Face)
14 – 18 Dec 2026	London, UK	USD 3495 per delegate

Introduction

As organizations increasingly rely on mobile technologies for productivity and communication, mobile devices and applications have become critical targets for cyberattacks. Weak security controls, unvetted apps, and insufficient policies can lead to data breaches, financial loss, and regulatory penalties.

This intensive 5-day course provides participants with the expertise to conduct thorough audits of mobile device and application security. From mobile operating systems and enterprise mobility management (EMM) to secure coding practices and threat detection, this training equips professionals with the tools and techniques to assess and strengthen mobile security posture across platforms.

Objectives

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

- Understand the architecture and risks associated with iOS and Android platforms
- Audit mobile device management (MDM) and BYOD policies
- Identify vulnerabilities in mobile apps and assess secure coding practices
- Evaluate encryption, authentication, and data leakage prevention controls
- Report findings and recommend remediation measures aligned with industry 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

- To mitigate growing risks associated with mobile device usage in corporate environments
- To comply with data protection regulations (e.g., GDPR, HIPAA) affecting mobile access
- To ensure secure mobile application development and deployment
- To understand audit methodologies tailored to mobile infrastructure and devices
- To improve enterprise-wide mobile threat detection and response capabilities

Target Audience

This program is designed for:

- IT auditors and cybersecurity auditors
- Mobile security engineers and IT risk managers
- Information security officers and compliance professionals
- App developers and QA/security testers
- Anyone responsible for auditing or managing mobile device security

Individual Benefits

Key competencies that will be developed include:

- Mobile operating system architecture and risk understanding
- Assessment of mobile apps for security and compliance
- Mobile policy evaluation (MDM, BYOD, corporate apps)
- Audit reporting techniques and evidence documentation
- Vulnerability testing and penetration simulation basics

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Reduced risk of data leakage and mobile-based cyberattacks
- Improved visibility and control over mobile devices and apps
- Stronger compliance posture with security policies and regulations
- Enhanced mobile incident response capabilities
- Strengthened collaboration between audit, IT, and development teams

Instructional Methodology

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

- Strategy Briefings: Overview of mobile threats, audit frameworks, and OS architecture
- Case Studies: Mobile security incidents, root causes, and lessons learned
- Workshops: Mobile app review, policy gap analysis, and audit plan development
- Peer Exchange: Group discussions on enterprise mobility challenges
- Tools: Mobile security audit templates, MDM checklists, test cases, and reporting formats

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 Mobile Ecosystems and Risk Landscape

- Module 1: Overview of Mobile Security Threats (07:30 – 09:30) • Mobile malware, data leakage, jailbreaking, and rogue apps • Mobile-specific attack vectors
- Module 2: iOS and Android Architecture (09:45 – 11:15) • Security models, sandboxing, app permissions, and OS updates
- Module 3: Workshop – Threat Mapping for Mobile Devices (11:30 – 01:00) • Identifying common vulnerabilities and entry points
- Module 4: Mobile Governance and Policy Frameworks (02:00 – 03:30) • MDM, BYOD, and enterprise security baselines

Day 2: Auditing Mobile Devices and Management Platforms

- Module 5: Mobile Device Management (MDM) Systems (07:30 – 09:30) • Policy configuration, encryption enforcement, and remote wipe
- Module 6: Compliance and Regulatory Alignment (09:45 – 11:15) • Auditing for GDPR, HIPAA, and PCI DSS on mobile endpoints
- Module 7: Workshop – MDM Configuration Review (11:30 – 01:00) • Evaluating security posture of MDM implementation
- Module 8: Network and Communication Security (02:00 – 03:30) • VPNs, secure tunneling, Wi-Fi controls, and mobile certificates

Day 3: Mobile Application Security

- Module 9: Secure Mobile Application Development (07:30 – 09:30) • OWASP Mobile Top 10 vulnerabilities and mitigation strategies
- Module 10: Static and Dynamic Analysis of Mobile Apps (09:45 – 11:15) • Testing tools and audit techniques
- Module 11: Workshop – Mobile App Audit Simulation (11:30 – 01:00) • Reviewing a mobile app for compliance and security
- Module 12: Secure APIs and Backend Connectivity (02:00 – 03:30) • Evaluating authentication, data transmission, and token security

Day 4: Incident Response and Forensics for Mobile

- Module 13: Mobile Incident Detection and Response (07:30 – 09:30) • Alerting, logging, and behavior monitoring
- Module 14: Mobile Forensics Basics (09:45 – 11:15) • Evidence acquisition, chain of custody, and forensic tools
- Module 15: Workshop – Simulated Mobile Incident Handling (11:30 – 01:00) • Response planning for a mobile data breach
- Module 16: Integrating Mobile Security into Enterprise Risk Strategy (02:00 – 03:30) • Governance, oversight, and policy alignment

Day 5: Audit Planning, Reporting, and Wrap-Up

- Module 17: Developing a Mobile Security Audit Plan (07:30 – 09:30) • Scope, objectives, stakeholders, and tools
- Module 18: Reporting and Communicating Audit Findings (09:45 – 11:15) • Structure, recommendations, and executive summaries
- Module 19: Workshop – Drafting a Mobile Security Audit Report (11:30 – 01:00) • Final exercise based on multi-platform scenario
- Module 20: Final Review and Certification (02:00 – 03:30) • Q&A, feedback, and post-training implementation plan

Certification

Participants will receive a Certificate of Completion in Mobile Security Audit, validating their ability to assess, report, and improve mobile security governance across devices, applications, and infrastructure.

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**

Follow us: **Facebook** **Twitter** **YouTube** **LinkedIn** **Instagram**

© Material published by MAWA Events shown here is copyrighted. All rights reserved. Any unauthorized copying, distribution, use, dissemination, downloading, storing (in any medium), transmission, reproduction or reliance in whole or any part of this course outline is prohibited and will constitute an infringement of copyright.