MAWA EVENTS

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

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

AI AND MACHINE LEARNING SECURITY AUDIT: REVIEWS THE SECURITY OF SYSTEMS UTILIZING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING.

""Assessing and Securing Intelligent Systems Through Risk-Based Auditing""

Schedule

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

Introduction

Artificial Intelligence (AI) and Machine Learning (ML) technologies are revolutionizing operations across all sectors—from finance to healthcare and national security. However, these intelligent systems introduce unique risks related to data integrity, algorithmic bias, adversarial attacks, and model governance.

This 5-day training is designed to equip IT auditors, cybersecurity professionals, and risk managers with the knowledge and tools to audit and secure AI and ML-based systems. Participants will learn how to identify threats, assess vulnerabilities, and ensure compliance with emerging AI security and ethical frameworks

Objectives

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

- Understand the architecture and lifecycle of AI and ML systems
- Identify AI/ML-specific risks, including data poisoning and adversarial inputs
- Evaluate controls over AI models, datasets, and algorithm transparency
- Conduct risk-based security audits of intelligent systems
- Align AI audits with standards, regulations, and ethical practices

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

- Stay ahead of the curve in AI risk management and security auditing
- Learn how to assess black-box algorithms and data-driven models
- Gain practical experience in auditing AI environments and toolchains
- Address emerging challenges around privacy, fairness, and accountability in AI
- Prepare for upcoming compliance requirements in AI governance

Target Audience

This program is designed for:

- IT and cybersecurity auditors
- Risk and compliance officers
- AI/ML engineers and data science leads
- Information security professionals
- Internal audit, governance, and assurance teams

Individual Benefits

Key competencies that will be developed include:

- AI/ML risk assessment and threat modeling
- Audit planning for AI-enabled environments
- Ethical AI principles and regulatory frameworks
- Security controls for training data, models, and inference pipelines
- Evaluation of AI system documentation, traceability, and explainability

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Strengthened oversight over AI-driven operations
- Improved risk mitigation for intelligent automation
- Compliance with AI-related laws, standards, and best practices
- Enhanced internal audit readiness for digital transformation
- Resilient, transparent, and accountable AI deployments

Instructional Methodology

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

- Strategy Briefings – AI architecture, threats, governance models
- Case Studies – AI failures, bias audits, and regulatory breaches
- Workshops – Conduct AI system audit planning, testing, and reporting
- Peer Exchange – Share experiences in auditing data-driven systems
- Tools – Checklists, AI audit templates, risk frameworks, and controls catalogues

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: AI & ML Technology Landscape and Audit Imperatives

- Module 1: Fundamentals of AI and Machine Learning (07:30 – 09:30) • AI types, ML lifecycle, and system components • Real-world use cases and audit significance
- Module 2: Risk Exposure in AI Systems (09:45 – 11:15) • Bias, explainability, adversarial threats, and data drift
- Module 3: Workshop – Identify Risks in a Sample AI System (11:30 – 01:00) • Analyze a system for vulnerabilities and weak controls

Day 2: Governance, Ethics, and Audit Standards

- Module 4: Ethical AI and Regulatory Landscape (07:30 – 09:30) • OECD principles, EU AI Act, ISO/IEC 23894:2023
- Module 5: AI Governance & Roles and Responsibilities (09:45 – 11:15) • AI steering committees, model documentation, auditability
- Module 6: Workshop – Audit Role Mapping in AI Governance (11:30 – 01:00) • Define roles for responsible AI oversight

Day 3: Data Management and Model Integrity Controls

- Module 7: Training Data and Input Risk Controls (07:30 – 09:30) • Data lineage, poisoning threats, versioning, and PII protection
- Module 8: ML Models and Algorithm Audit Techniques (09:45 – 11:15) • Version control, interpretability, robustness testing
- Module 9: Workshop – Evaluate a Model Validation Report (11:30 – 01:00) • Audit model documentation and controls coverage

Day 4: AI System Testing and Audit Execution

- Module 10: AI Audit Planning and Scope Definition (07:30 – 09:30) • Selecting objectives, tools, and audit focus areas
- Module 11: Control Testing Techniques (09:45 – 11:15) • Black-box vs white-box testing, simulation, red teaming
- Module 12: Workshop – Draft AI Security Audit Plan (11:30 – 01:00) • Create an audit scope and checklist for an AI deployment

Day 5: Audit Reporting and Future Trends

- Module 13: Reporting AI Audit Findings and Recommendations (07:30 – 09:30) • Communicating risks, controls gaps, and remediation
- Module 14: Trends in AI Security and Governance (09:45 – 11:15) • AI in cybersecurity, explainable AI, and audit automation
- Module 15: Final Workshop – Present an AI Audit Case (11:30 – 01:00) • Deliver an audit summary with findings and risk rating

Certification

Participants will receive a Certificate of Completion in AI and Machine Learning Security Audit, validating their capability to assess the design, governance, and security of AI-driven systems using internationally recognized audit 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**