MAWA EVENTS

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

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

INCIDENT RESPONSE AUDIT: REVIEWS THE EFFECTIVENESS OF AN ORGANIZATION\'S INCIDENT RESPONSE PLAN AND PROCESSES

""Evaluating the Readiness, Effectiveness, and Governance of Cybersecurity Incident Response Programs""

Schedule

Date	Venue	Fees (Face-to-Face)
21 – 25 Sep 2026	London, UK	USD 3495 per delegate

Introduction

Cybersecurity incidents—including ransomware attacks, data breaches, and system outages—are increasing in scale and complexity. Organizations must be prepared to respond rapidly and effectively to minimize damage and ensure business continuity. A comprehensive incident response audit ensures that your response plans, roles, and technical capabilities are functioning as intended.

This intensive 5-day course equips cybersecurity professionals, internal auditors, and risk managers with the knowledge and techniques to audit an organization’s incident response (IR) readiness. Participants will learn how to assess IR policies, plans, response procedures, post-incident reviews, and alignment with standards like NIST 800-61, ISO 27035, and GDPR breach obligations.

Objectives

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

- Understand incident response lifecycle phases and regulatory requirements
- Plan and execute an incident response audit across IT and business functions
- Evaluate IR governance, escalation procedures, and communications protocols
- Assess detection capabilities, log management, and response effectiveness
- Document findings, prioritize gaps, and recommend improvements for resilience

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 verify that your organization is prepared to detect, contain, and recover from cyber incidents
- To identify gaps in response workflows, documentation, and responsibilities
- To assess the maturity of IR practices against international standards
- To improve executive visibility and accountability for cybersecurity risk
- To reduce financial, operational, and reputational damage from cyber threats

Target Audience

This program is designed for:

- IT and cybersecurity auditors
- Information security officers and SOC managers
- Compliance, governance, and risk management professionals
- IT operations, incident handlers, and response coordinators
- Any stakeholder involved in incident response planning or review

Individual Benefits

Key competencies that will be developed include:

- Planning and conducting IR audits
- Evaluating detection, escalation, containment, and recovery controls
- Reviewing incident logs, communications, and after-action reviews
- Testing IR scenarios and compliance with breach regulations
- Producing detailed, risk-based audit reports and remediation plans

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved incident preparedness and cyber resilience
- Reduced response time and data breach impact
- Stronger alignment with ISO 27035, NIST CSF, and GDPR breach protocols
- Auditable IR plans, playbooks, and recovery documentation
- Enhanced collaboration between cybersecurity, legal, and executive teams

Instructional Methodology

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

- Strategy Briefings – IR frameworks, audit objectives, and regulatory standards
- Case Studies – Analysis of real-world cyber incidents and response failures
- Workshops – IR playbook reviews, gap analysis, and incident simulation audits
- Peer Exchange – Cross-industry challenges and IR program benchmarking
- Tools – Audit checklists, evidence logs, response templates, and 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

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: Foundations of Incident Response and Audit Planning

- Module 1: Understanding the Incident Response Lifecycle (07:30 – 09:30) • NIST and ISO phases: prepare, detect, respond, recover • Common cyber incidents and impact categories
- Module 2: IR Policy and Governance Review (09:45 – 11:15) • Reviewing incident response policies, scope, and roles • Escalation chains and legal/regulatory requirements
- Module 3: Planning the IR Audit (11:30 – 01:00) • Defining audit scope, objectives, and risk focus areas • Stakeholder interviews and document checklist
- Module 4: Workshop – IR Audit Planning Exercise (02:00 – 03:30) • Build a tailored IR audit plan for a case scenario

Day 2: Detection, Identification, and Logging Controls

- Module 1: Detection Capabilities Audit (07:30 – 09:30) • Log management, SIEM, IDS/IPS, endpoint monitoring • Alert thresholds, tuning, and analyst coverage
- Module 2: Incident Logging and Documentation (09:45 – 11:15) • Incident tickets, log files, timestamps, and root cause fields • Evidence integrity and chain of custody
- Module 3: Initial Triage and Classification (11:30 – 01:00) • Severity levels and prioritization protocols • False positives and escalation review
- Module 4: Simulation – Analyze Alert and Log Samples (02:00 – 03:30) • Identify audit issues in monitoring and classification

Day 3: Containment, Eradication, and Recovery

- Module 1: Containment Strategies and Playbooks (07:30 – 09:30) • Short-term and long-term containment techniques • Role of SOC and IT teams in isolation procedures
- Module 2: Eradication and Forensic Analysis (09:45 – 11:15) • Malware removal, patching, and threat hunting • Use of forensic tools and evidence validation
- Module 3: System and Business Recovery (11:30 – 01:00) • Restoration of services, backups, and rollback checks • Validation before closing incidents
- Module 4: Workshop – Audit of Recovery Actions (02:00 – 03:30) • Assess response logs and recovery evidence

Day 4: Communications, Reporting, and Post-Incident Review

- Module 1: Stakeholder and Regulator Communication (07:30 – 09:30) • Notification protocols: executive, legal, customers, authorities • GDPR, HIPAA, and other breach regulations
- Module 2: Incident Reporting and Documentation (09:45 – 11:15) • Templates, tracking sheets, and audit trail completeness • Metrics and KPIs
- Module 3: Lessons Learned and Program Improvement (11:30 – 01:00) • Post-incident reviews, corrective actions, and tracking
- Module 4: Simulation – Review a Breach Response Case (02:00 – 03:30) • Identify audit gaps and provide improvement recommendations

Day 5: Maturity Assessment, Continuous Monitoring, and Reporting

- Module 1: IR Maturity Models and Benchmarks (07:30 – 09:30) • Defining maturity levels across processes and capabilities • CMMI, NIST, and proprietary models
- Module 2: Continuous IR Improvement and Testing (09:45 – 11:15) • Tabletop exercises, red teaming, and breach drills • Testing audit readiness across departments
- Module 3: Audit Reporting and Remediation (11:30 – 01:00) • Prioritizing gaps, writing audit reports, and managing risk
- Module 4: Final Presentations and Certification (02:00 – 03:30) • Group presentations, course feedback, and certification ceremony

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 Incident Response Audit, confirming their ability to assess, monitor, and improve cybersecurity incident response capabilities aligned with global 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**

© 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.