MAWA EVENTS

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

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

IT TRAINING AND AWARENESS AUDIT: ASSESSES THE LEVEL OF CYBERSECURITY AWARENESS AND TRAINING AMONG EMPLOYEES

"Auditing Cybersecurity Awareness and Training Programs to Strengthen the Human Firewall"

Schedule

Date	Venue	Fees (Face-to-Face)
23 – 27 Nov 2026	London – UK	USD 3495 per delegate

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

Introduction

With human error being one of the leading causes of cybersecurity breaches, employee awareness and training are critical components of an organization\'s information security defense. However, without proper auditing, the effectiveness of these programs often goes unmeasured.

This course provides professionals with the tools to assess cybersecurity training programs, awareness initiatives, and compliance with security policies. Participants will learn how to evaluate the scope, delivery, impact, and governance of IT training efforts to ensure they effectively reduce risk and promote a security-conscious culture.

Objectives

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

- Assess the adequacy and effectiveness of cybersecurity awareness and IT training programs
- Evaluate policy compliance, learning coverage, and user engagement
- Measure training outcomes using metrics, testing, and behavioral indicators
- Review third-party training vendors and e-learning platforms for content quality
- Develop audit reports with actionable insights to improve awareness initiatives

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

- Help your organization build a stronger “human firewall” against cyber threats
- Ensure compliance with data protection regulations and training mandates
- Identify gaps in IT policy communication and user understanding
- Evaluate content quality, training frequency, and risk coverage
- Provide leadership with assurance on cybersecurity readiness

Target Audience

This program is designed for:

- Internal and IT auditors
- Cybersecurity awareness and training managers
- GRC and compliance officers
- HR and L&D professionals responsible for IT training
- Information security and risk management personnel

Individual Benefits

Key competencies that will be developed include:

- Auditing cybersecurity awareness and behavioral change programs
- Reviewing training frameworks and assessing learning coverage
- Identifying social engineering risks and awareness gaps
- Applying compliance standards (e.g., ISO/IEC 27001, NIST, GDPR)
- Crafting evidence-based reports with measurable insights

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved assurance over employee cybersecurity readiness
- More targeted and risk-aligned training content
- Reduced risk of human-factor data breaches
- Stronger compliance with regulatory awareness requirements
- Better coordination between cybersecurity, HR, and compliance functions

Instructional Methodology

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

- Strategy Briefings – Frameworks, compliance standards, and behavioral risk models
- Case Studies – Real-world breaches linked to awareness failures
- Workshops – Training evaluation tools, surveys, and testing simulations
- Peer Exchange – Group discussions on training effectiveness and improvement
- Tools – Audit checklists, e-learning scorecards, and awareness maturity models

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 Awareness and Training Auditing

- Module 1: Cybersecurity and Human Risk (07:30 – 09:30) • Role of human behavior in cybersecurity breaches • Phishing, social engineering, and insider threat trends
- Module 2: Frameworks for Training and Awareness (09:45 – 11:15) • ISO 27001, NIST 800-50, GDPR training mandates • Organizational learning vs. compliance-based training
- Module 3: Workshop – Program Mapping and Gap Analysis (11:30 – 01:00) • Assess a sample training program's coverage and gaps
- Module 4: Peer Exchange – Awareness Culture Challenges (02:00 – 03:30) • Group discussion on behavioral barriers and leadership support

Day 2: Scoping and Planning the Awareness Audit

- Module 5: Awareness Audit Scope and Criteria (07:30 – 09:30) • Defining objectives, engagement scope, and control areas • User groups, training cycles, and communication channels
- Module 6: Policy Communication and Reinforcement (09:45 – 11:15) • IT usage policies, acceptable behavior, and password protocols • Evaluating visibility and understanding
- Module 7: Workshop – Audit Plan for Cyber Awareness (11:30 – 01:00) • Build an audit plan for an organization-wide training program
- Module 8: Case Study – Untrained Employees and Data Loss (02:00 – 03:30) • Learn from a breach rooted in weak policy awareness

Day 3: Evaluation Tools and Testing Techniques

- Module 9: Metrics and KPIs for Awareness (07:30 – 09:30) • Click rates, quiz scores, reporting rates, and phishing simulations • Measuring change in behavior over time
- Module 10: Reviewing Content and Delivery Methods (09:45 – 11:15) • E-learning, in-person, and microlearning evaluations • Third-party vendor assessment
- Module 11: Workshop – Scoring Training Content (11:30 – 01:00) • Use a checklist to evaluate training modules
- Module 12: Peer Discussion – Training Impact Assessment (02:00 – 03:30) • Group insights on tools and results tracking

Day 4: Stakeholder Interviews and Cultural Assessment

- Module 13: Conducting Interviews and Surveys (07:30 – 09:30) • Techniques for interviewing staff, managers, and IT trainers • Awareness perception and behavioral audits
- Module 14: Evaluating Organizational Culture and Accountability (09:45 – 11:15) • Culture of reporting, peer reinforcement, and management support
- Module 15: Workshop – Simulated Staff Interview Session (11:30 – 01:00) • Role-play interviews and survey feedback review
- Module 16: Case Study – Organizational Blind Spots (02:00 – 03:30) • How cultural gaps caused awareness failure

Day 5: Reporting, Recommendations, and Audit Closure

- Module 17: Developing the Awareness Audit Report (07:30 – 09:30) • Structure, findings, and improvement recommendations
- Module 18: Communicating Results to Executives (09:45 – 11:15) • Reporting behavioral risks and KPIs with clarity
- Module 19: Final Project – Awareness Audit Simulation (11:30 – 01:00) • Plan and present audit findings on a sample training program
- Module 20: Wrap-Up, Feedback, and Certification (02:00 – 03:30) • Course debrief and certification

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 IT Training and Awareness Audit, validating their ability to audit, evaluate, and improve cybersecurity training and awareness programs to enhance organizational resilience.

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**