MAWA EVENTS

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

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

ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

""Building a Robust Information Security Management System for Risk Mitigation and Compliance""

Schedule

Date	Venue	Fees (Face-to-Face)
17 – 21 May 2026	Doha, Qatar	USD 3495 per delegate

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

Introduction

ISO/IEC 27001 is the internationally recognized standard for Information Security Management Systems (ISMS). This 5-day course is designed to help professionals develop a thorough understanding of ISMS principles, how to implement and maintain an effective information security management system, and how to ensure compliance with ISO/IEC 27001 standards. Participants will learn how to safeguard sensitive information, manage security risks, and maintain the confidentiality, integrity, and availability of data.

Through a combination of theoretical learning, case studies, and practical exercises, participants will gain the skills and knowledge to implement and audit ISMS effectively, driving continuous improvement in information security practices across their organization.

Objectives

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

- Understand the ISO/IEC 27001 framework and its requirements for information security management.
- Implement an Information Security Management System (ISMS) in compliance with ISO/IEC 27001 standards.
- Conduct risk assessments and identify potential security threats to information assets.
- Develop and implement policies and controls to mitigate information security risks.
- Lead internal audits to evaluate the effectiveness of ISMS and ensure continuous improvement.
- Ensure organizational compliance with information security regulations and best 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

- Gain comprehensive knowledge of ISO/IEC 27001 and its application in managing information security.
- Learn how to design, implement, and maintain an effective ISMS to protect sensitive data and ensure compliance.
- Understand how to assess and mitigate security risks across information systems.
- Develop auditing skills to evaluate and monitor ISMS effectiveness and continuous improvement.
- Strengthen your organization’s security posture and build trust with customers, regulators, and stakeholders.
- Master the principles and tools required to achieve ISO/IEC 27001 certification and maintain compliance.

Target Audience

This program is designed for:

- Information security professionals, risk managers, and compliance officers
- IT managers and system administrators responsible for maintaining secure systems
- Internal auditors and professionals involved in auditing or managing ISMS
- Senior executives and managers seeking to understand and implement ISO/IEC 27001 in their organization
- Anyone seeking to become certified as ISO/IEC 27001 Lead Implementers or Lead Auditors

Individual Benefits

Key competencies that will be developed include:

- Mastery of ISO/IEC 27001 standards for implementing an effective ISMS.
- Skills in conducting risk assessments and implementing controls to mitigate security risks.
- Expertise in developing, implementing, and maintaining information security policies.
- Proficiency in auditing ISMS to ensure compliance and continuous improvement.
- Ability to communicate and manage information security across an organization effectively.

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved security management capabilities to protect sensitive data and information.
- Stronger organizational compliance with ISO/IEC 27001 and other security regulations.
- Enhanced ability to identify, assess, and mitigate information security risks.
- More effective internal audits and assessments of ISMS performance.
- Increased trust and credibility with stakeholders through strong information security practices.

Instructional Methodology

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

- Strategy Briefings – In-depth sessions on ISO/IEC 27001, risk management, and information security principles.
- Case Studies – Real-world examples of implementing ISMS and achieving ISO/IEC 27001 certification.
- Workshops – Hands-on exercises for designing and implementing ISMS policies and controls.
- Peer Exchange – Group discussions to share experiences and best practices in information security.
- Tools – Practical tools and templates to help implement and maintain an ISMS.

MAWA EVENTS

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

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

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: 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 ISO/IEC 27001 and ISMS

- Module 1: Overview of ISO/IEC 27001 and ISMS (07:30 – 09:30)
- The importance of information security management
- Key concepts and principles of ISO/IEC 27001
- Benefits of implementing an ISMS in the organization
- Module 2: Structure of ISO/IEC 27001 and ISMS Requirements (09:45 – 11:15)
- The structure and clauses of ISO/IEC 27001
- Understanding the Plan-Do-Check-Act (PDCA) model for ISMS
- Key requirements of ISO/IEC 27001 for effective implementation
- Module 3: Context of the Organization and Leadership Commitment (11:30 – 01:00)
- Determining the context of the organization and stakeholders' needs
- The role of leadership in promoting a culture of information security
- Defining roles, responsibilities, and resources for ISMS

Day 2: Risk Management and Information Security Assessment

- Module 1: Risk Assessment and Risk Treatment (07:30 – 09:30)
- Conducting a risk assessment: identifying and evaluating information security risks
- Developing a risk treatment plan to mitigate risks
- Applying risk management techniques to ISMS
- Module 2: Information Security Controls (09:45 – 11:15)
- Understanding ISO/IEC 27002 controls for information security
- Developing policies and procedures for effective risk management
- Selecting and implementing appropriate security controls
- Module 3: Implementing and Operating ISMS (11:30 – 01:00)
- Developing and implementing ISMS policies, procedures, and controls
- Establishing an incident response plan and business continuity plan
- Implementing controls for asset management, access control, and cryptography

Day 3: Monitoring and Measuring ISMS Performance

- Module 1: Monitoring and Measuring ISMS Performance (07:30 – 09:30)
- Key performance indicators (KPIs) for ISMS effectiveness
- Continuous monitoring, review, and improvement of ISMS performance
- Internal audits to assess compliance and effectiveness of ISMS
- Module 2: Conducting Internal Audits (09:45 – 11:15)
- Planning and conducting internal audits for ISMS
- Reporting audit findings and nonconformities
- Corrective and preventive actions for improving ISMS
- Module 3: Management Review and Continuous Improvement (11:30 – 01:00)
- The role of management review in the success of ISMS
- Continuous improvement processes for maintaining ISMS effectiveness
- Ensuring long-term success and sustainability of ISMS

Day 4: Certification and Compliance

-

Module 1: ISO/IEC 27001 Certification Process (07:30 – 09:30)

- Steps to achieving ISO/IEC 27001 certification
- Preparing for certification audits and assessments
- Roles of external auditors and certification bodies
- Module 2: Maintaining Compliance and Managing Change (09:45 – 11:15)
- Maintaining ISO/IEC 27001 compliance after certification
- Managing changes to ISMS and ensuring continued effectiveness
- Document control and versioning in ISMS
- Module 3: Case Study and Practical Application (11:30 – 01:00)
- Analyzing real-world examples of successful ISMS implementations
- Workshop on designing and implementing an ISMS
- Reviewing the challenges and best practices

Day 5: ISMS Implementation Workshop and Wrap-Up

- Module 1: ISMS Implementation Workshop (07:30 – 09:30)
- Practical exercise: Developing an ISMS implementation plan
- Group activity to design and present ISMS policies and controls
- Module 2: Preparing for Certification and Continuous Improvement (09:45 – 11:15)
- Final preparation for ISO/IEC 27001 certification audit
- Maintaining an ongoing improvement culture within the organization
- Module 3: Final Q&A and Course Conclusion (11:30 – 01:00)
- Open Q&A session with course instructors
- Recap of key takeaways
- Course wrap-up and certificate distribution

Certification

Upon completing the training course, participants will receive a Certificate of Completion in ISO/IEC 27001 Information Security Management System (ISMS), recognizing their ability to implement, audit, and maintain an effective ISMS, ensuring compliance with ISO/IEC 27001 standards and safeguarding organizational information security.

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**

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.