QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1942

# Information Security Management System (ISMS) & ISO 27001 Training Course

CYBERSECURITY & INFORMATION SECURITY
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION
**5 Days**

DELIVERY
**Classroom**

## Course Overview

The Information Security Management System (ISMS) & ISO 27001 Training Course provides a comprehensive and practical understanding of how organizations can establish, implement, maintain, and continually improve an effective Information Security Management System in alignment with ISO/IEC 27001 requirements. The course focuses on building a structured approach to protecting information assets, managing information security risks, and strengthening organizational resilience.

Participants will explore the key principles and components of an ISMS, including organizational context, leadership, information security objectives, risk assessment, risk treatment, documented information, operational controls, performance evaluation, internal audit, management review, and continual improvement.

The course also examines how ISO/IEC 27001 can be integrated with broader organizational governance, enterprise risk management, cybersecurity programs, business continuity, privacy, compliance, and third-party risk management. Participants will learn how to translate the standard's requirements into practical policies, processes, controls, responsibilities, and measurable security outcomes.

Through practical exercises, risk assessment workshops, control-mapping activities, ISMS documentation exercises, internal audit simulations, and implementation planning, participants will develop the capabilities required to establish a sustainable ISMS, identify compliance gaps, prepare for audits, and drive continual information security improvement.

## Objectives

- By the end of the course, participants will be able to:
- Analyze the purpose, structure, and principles of an Information Security Management System.
- Interpret the key requirements of ISO/IEC 27001 and their organizational implications.
- Establish the scope and context of an ISMS.
- Identify information assets, stakeholders, security requirements, and organizational risks.
- Conduct structured information security risk assessments.

- Develop risk treatment strategies and security objectives.
- Design information security policies, procedures, and documented processes.
- Map security controls to identified risks and organizational requirements.
- Establish processes for monitoring, measuring, and evaluating ISMS performance.
- Plan and conduct effective internal ISMS audits.
- Identify nonconformities and develop corrective action plans.
- Prepare organizations for management reviews and external certification audits.
- Integrate the ISMS with cybersecurity, business continuity, compliance, and enterprise risk management.
- Establish continual improvement mechanisms for information security.
- Develop a practical roadmap for implementing and maintaining an ISO/IEC 27001-aligned ISMS.

## Who Should Attend

This course is designed for information security professionals, cybersecurity specialists, IT managers, information security managers, ISMS coordinators, security governance professionals, risk managers, compliance officers, internal auditors, and professionals responsible for implementing or maintaining information security management systems.

It is also suitable for business continuity professionals, quality and governance specialists, enterprise risk professionals, technology assurance teams, security architects, data protection professionals, and managers involved in organizational security, regulatory compliance, audit readiness, and information risk management.

The course is particularly valuable for organizations preparing to establish, improve, or maintain an ISO/IEC 27001-aligned information security management system and for professionals who need a practical understanding of how information security governance, risk management, controls, documentation, auditing, and continual improvement work together.

## Learning Outcomes

- By the end of the course, participants will be able to:
- Explain the structure and fundamental principles of an ISMS.
- Interpret the main requirements of ISO/IEC 27001.
- Define an appropriate ISMS scope and organizational context.
- Identify information assets and information security requirements.
- Conduct information security risk assessments.
- Evaluate risks based on likelihood, impact, and organizational priorities.
- Develop risk treatment plans and information security objectives.
- Establish appropriate information security policies and documented procedures.
- Map security controls to information security risks and organizational requirements.
- Develop and maintain ISMS documentation and evidence.
- Monitor and evaluate information security performance.
- Conduct internal ISMS audits and document audit findings.
- Manage nonconformities, corrective actions, and improvement opportunities.
- Prepare for management reviews and external certification assessments.
- Develop an integrated ISMS implementation and continual improvement roadmap.

## Course Outline

DAY 01

### ISMS Foundations, ISO 27001, and Organizational Context

- Understanding information security management systems.
- Purpose and business value of an ISMS.
- Overview of ISO/IEC 27001 and its management-system approach.
- Key principles of information security governance.
- Understanding organizational context and interested parties.
- Determining the scope of the ISMS.
- Information security responsibilities and leadership.
- Establishing information security policies and objectives.

DAY 01 — CONTINUED

- Aligning the ISMS with organizational strategy and risk appetite.
- Information security governance structures.
- Understanding the ISMS lifecycle and continual improvement approach.

**PRACTICAL APPLICATION**

Define the organizational context and draft an ISMS scope, governance structure, and initial information security objectives for a representative organization.

DAY 02

## Information Security Risk Assessment and Risk Treatment

- Principles of information security risk management.
- Identifying information assets and critical business processes.
- Identifying threats, vulnerabilities, and security risks.
- Risk identification and analysis methodologies.
- Evaluating likelihood and business impact.
- Establishing risk evaluation criteria.
- Risk acceptance and ownership.
- Developing risk treatment options.
- Selecting appropriate security controls.
- Developing risk treatment plans.
- Establishing risk registers and maintaining risk information.
- Aligning risk treatment with organizational priorities.

**PRACTICAL APPLICATION**

Conduct an information security risk assessment, develop a risk register, evaluate identified risks, and prepare a risk treatment plan.

DAY 03

## ISMS Controls, Policies, and Implementation

- Understanding the relationship between risks, controls, and ISMS requirements.
- Information security policy framework.
- Access control and identity security.
- Asset management and information classification.
- Cryptography and data protection.
- Physical and environmental security.
- Operational security and secure technology management.
- Communications and network security.
- Supplier and third-party security.
- Incident management and information security events.
- Business continuity and information security resilience.
- Security awareness and organizational competence.
- Documented information and evidence management.

> **PRACTICAL APPLICATION**
>
> Develop a control-mapping exercise linking identified information security risks to appropriate controls, policies, responsibilities, and implementation evidence.

DAY 04

## ISMS Performance, Internal Audit, and Management Review

- Monitoring and measurement of ISMS performance.
- Information security objectives and performance indicators.
- Control effectiveness assessment.
- Internal audit principles and planning.
- Developing an ISMS audit program.
- Preparing audit criteria, scope, and evidence requirements.
- Conducting internal audit interviews and evidence reviews.
- Identifying findings and nonconformities.

DAY 04 — CONTINUED

- Root cause analysis and corrective actions.
- Management review requirements and inputs.
- Evaluating ISMS effectiveness and suitability.
- Preparing for external certification audits.

**PRACTICAL APPLICATION**

Conduct a simulated ISMS internal audit, document findings and nonconformities, perform root cause analysis, and develop corrective action plans.

DAY 05

## ISO 27001 Implementation, Certification Readiness, and Continual Improvement

- Building an ISO/IEC 27001 implementation program.
- Developing an ISMS implementation roadmap.
- Establishing governance, roles, and responsibilities.
- Managing implementation resources and organizational change.
- Addressing ISMS gaps and prioritizing corrective actions.
- Certification readiness assessment.
- Preparing documentation and audit evidence.
- Managing external audit activities.
- Maintaining the ISMS after implementation.
- Continual improvement and performance enhancement.
- Integrating the ISMS with enterprise risk management and cybersecurity.
- Linking information security with business continuity and organizational resilience.
- Establishing a sustainable ISMS operating model.

**FINAL WORKSHOP**

Develop an integrated ISO/IEC 27001-aligned ISMS implementation and improvement roadmap covering organizational context, scope, risk assessment, risk treatment, policies, controls, documentation, performance measurement, internal audit, management review, certification readiness, corrective actions, and continual improvement.

## Register or Request More Information

Course page: https://quest-training.com/courses/information-security-management-system-isms-iso-27001-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440