INFOSECTRAIN

ISO 27001:2022

Lead Implementer

Training and Certification

www.infosectrain.com

Course Highlights

- 32-Hour Instructor-led Training
- Flexible Schedule
- Immersive Learning
- Highly Interactive and Dynamic Sessions
- Learn with Real-World Scenarios
- Authorized Training Partner
- Career Guidance and Mentorship
- Extended Post Training Support
- Access to Recorded Sessions

About Course

The ISO 27001 ISMS Lead Implementer Training Course from InfosecTrain is a comprehensive program designed to help participants develop the necessary skills to support organizations in implementing and managing an Information Security Management System (ISMS) based on the ISO/IEC 27001:2022 standard. The course also covers best practices for implementing information security controls from all areas of ISO/IEC 27002. Upon completing the course, participants will thoroughly understand how to identify and mitigate information security risks, develop policies and procedures to ensure compliance with relevant laws and regulations and implement effective security controls to protect against cyber threats.

Course Objectives

- Explain the fundamental concepts and principles of an Information Security Management System (ISMS) based on ISO/IEC 27001.
- Interpret the ISO/IEC 27001 requirements for an ISMS from an implementer’s perspective.
- Initiate and plan the implementation of an ISMS based on ISO/IEC 27001 by utilizing IMS2 Methodology and other best practices.
- Support an organization in operating, maintaining, and continually improving an ISMS based on ISO/IEC 27001.
- Prepare an organization to undergo a third-party certification audit.

Target Audience

- Project Managers and Consultants who are involved in and concerned with implementing an ISMS.
- Expert advisors seeking to master the implementation of an ISMS.
- Individuals responsible for ensuring conformity to information security requirements within an organization.
- Members of an ISMS implementation team.

Pre-Requisites

It is required to have a fundamental understanding of Information Security Management Systems (ISMS) and the ISO/IEC 27001 standard.

Exam Information

We provide Exams with **TUV & IGC**

For more details, connect with our experts.

Course Content

Introduction to ISO/IEC 27001 and initiation of an ISMS

Section 1: Training course objectives and structure

- Introduction
- General information
- Learning objectives
- Educational approach
- Examination and certification

Section 2: Standards and regulatory frameworks

- What is ISO?
- The ISO/IEC 27000 family of standards
- Advantages of ISO/IEC 27001

Section 3: Information Security Management System (ISMS)

- Definition of a management system
- Management system standards
- Integrated management systems
- Definition of an ISMS
- Process approach
- Overview — Clauses 4 to 10
- Overview — Annex A

Section 4: Fundamental information security concepts and principles

- Information and asset
- Information security
- Availability, confidentiality, and integrity
- Vulnerability, threat, and impact
- Information security risk
- Classification of security controls

Section 5: Initiation of the ISMS implementation

- Define the approach to the ISMS implementation
- Proposed implementation approaches
- Application of the proposed implementation approaches
- Choose a methodological framework to manage the implementation of an ISMS
- Approach and methodology
- Alignment with best practices

Section 6: Understanding the organization and its context

- Mission, objectives, values, and strategies of the organization
- ISMS objectives
- Preliminary scope definition
- Internal and external environment
- Key processes and activities
- Interested parties
- Business requirements

Section 7: ISMS scope

- Boundary of the ISMS
- Organizational boundaries
- Information security boundaries
- Physical boundaries
- ISMS Scope statement

Planning the implementation of an ISMS

Section 8: Leadership and project approval

- Business case
- Resource requirements
- ISMS project plan
- ISMS project team
- Management approval

Section 9: Organizational structure

- Organizational structure
- Information security coordinator
- Roles and responsibilities of interested parties
- Roles and responsibilities of key committees

Section 10: Analysis of the existing system

- Determine the current state
- Conduct the gap analysis
- Establish maturity targets
- Publish a gap analysis report

Section 11: Information security policy

- Types of policies
- Policy models
- Information security policy
- Specific security policies
- Management policy approval
- Publication and dissemination
- Training and awareness sessions
- Control, evaluation, and review

Section 12: Risk management

- ISO/IEC 27005
- Risk assessment approach
- Risk assessment methodology
- Risk identification
- Risk estimation
- Risk evaluation
- Risk treatment
- Residual risk

Section 13: Statement of Applicability

- Drafting the Statement of Applicability
- Management approval
- Review and selection of the applicable information security controls
- Justification of selected controls
- Justification of excluded controls

Implementation of an ISMS

Section 14: Documented information management

- Value and types of documented information
- Master list of documented information
- Creation of templates
- Documented information management process
- Implementation of a documented information management system
- Management of records

Section 15: Selection and design of controls

- Organization’s security architecture
- Preparation for the implementation of controls
- Design and description of controls

Section 16: Implementation of controls

- Implementation of security processes and controls
- Introduction of Annex A controls

Section 17: Trends and technologies

- Big data
- The three V’s of big data
- Artificial intelligence
- Machine learning
- Cloud computing
- Outsourced operations
- The impact of new technologies in information security

Section 18: Communication

- Principles of an efficient communication strategy
- Information security communication process
- Establishing communication objectives
- Identifying interested parties
- Planning communication activities
- Performing a communication activity
- Evaluating communication

Section 19: Competence and awareness

- Competence and people development
- Difference between training, awareness, and communication
- Determine competence needs
- Plan the competence development activities
- Define the competence development program type and structure
- Training and awareness programs
- Provide the trainings
- Evaluate the outcome of trainings

Section 20: Security operations management

- Change management planning
- Management of operations
- Resource management
- ISO/IEC 27035-1 and ISO/IEC 27035-2
- ISO/IEC 27032
- Information security incident management policy
- Process and procedure for incident management
- Incident response team
- Incident management security controls
- Forensics process
- Records of information security incidents
- Measure and review of the incident management process

ISMS monitoring, continual improvement, and preparation for the certification audit

Section 21: Monitoring, measurement, analysis, and evaluation

- Determine measurement objectives
- Define what needs to be monitored and measured
- Establish ISMS performance indicators
- Report the results

Section 22: Internal audit

- What is an audit?
- Types of audits
- Create an internal audit program
- Designate a responsible person
- Establish independence, objectivity, and impartiality
- Plan audit activities
- Perform audit activities
- Follow up on nonconformities

Section 23: Management review

- Preparing a management review
- Conducting a management review
- Management review outputs
- Management review follow-up activities

Section 24: Treatment of nonconformities

- Root-cause analysis process
- Root-cause analysis tools
- Corrective action procedure
- Preventive action procedure

Section 25: Continual improvement

- Continual monitoring process
- Maintenance and improvement of the ISMS
- Continual update of the documented information
- Documentation of the improvements

Section 26: Preparing for the certification audit

- Selecting the certification body
- Preparing for the certification audit
- Stage 1 audit
- Stage 2 audit
- Follow-up audit
- Certification decision

INFOSECTRAIN

Educate. Excel. Empower.

www.infosectrain.com | sales@infosectrain.com