INFOSECTRAIN

ISO/IEC 27001

LEAD IMPLEMENTER

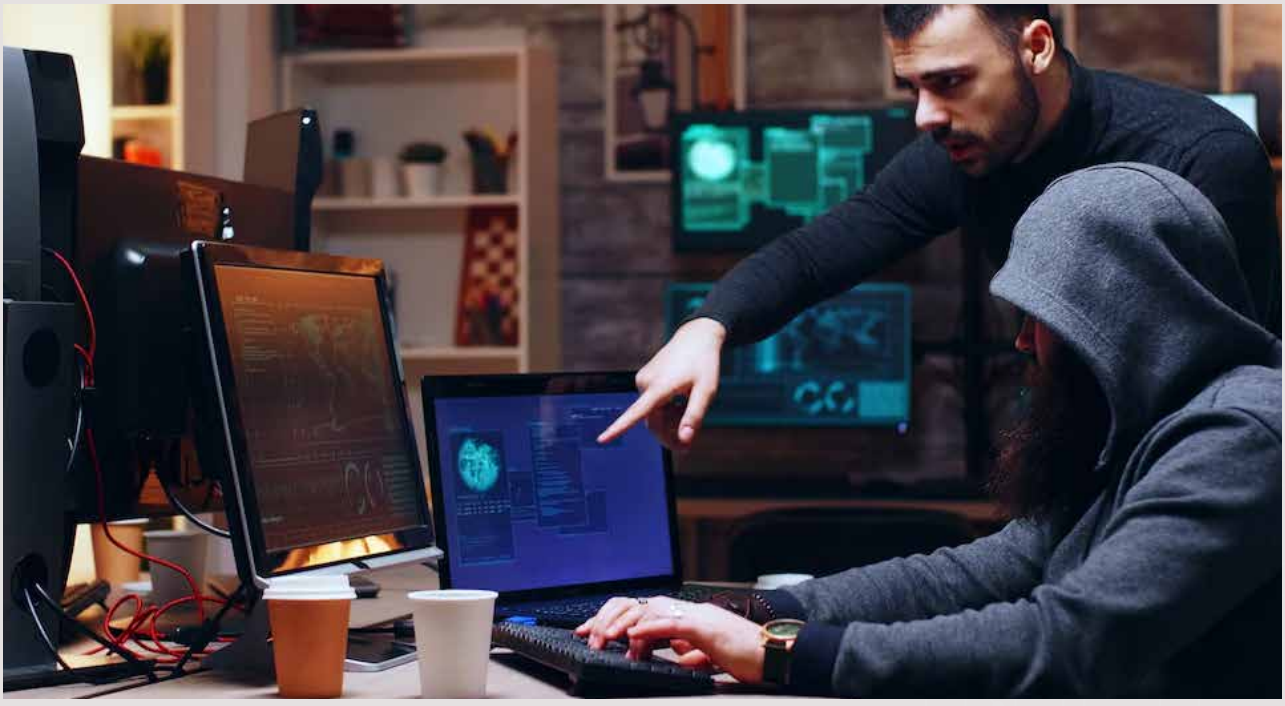
TRAINING & CERTIFICATION

PECB INITIATE PARTNER

TÜVRheinland® Precisely Right.

Overview

Certified ISO 27001 ISMS Lead Implementer Training Course has intensive course enables participants to develop the necessary expertise to support an organization in implementing and managing an Information Security Management System (ISMS) based on ISO/IEC 27001:2013. Participants will also gain a thorough understanding of best practices used to implement information security controls from all areas of ISO/IEC 27002. ISO 27001 Lead Implementer Training & Certification is consistent with the project management practices established in ISO 10006 (Quality Management Systems – Guidelines for Quality Management in Projects). This training is also fully compatible with ISO/IEC 27003 (Guidelines for the Implementation of ISMS), ISO/IEC 27004 (Measurement of Information Security) and ISO/IEC 27005 (Risk Management in Information Security).



Target Audience

- Project managers or consultants wanting to prepare and to support an organization in the implementation of an Information Security Management System (ISMS)
- ISO/IEC 27001 auditors who wish to fully understand the Information Security Management System implementation process
- CxO and Senior Managers responsible for the IT governance of an enterprise and the management of its risks
- Members of an information security team
- Expert advisors in information technology
- Technical experts wanting to prepare for an information security function or for an ISMS project management function

Pre-Requisites

- ISO/IEC 27001 Foundation Certification or a basic knowledge of ISO/IEC 27001 is recommended.

Course Objectives

- Introduction to management systems and the process approach Presentation of the standards ISO/IEC 27001, ISO 27002 and ISO 27003 and regulatory framework
- Fundamental principles of Information Security
- Preliminary analysis and establishment of the level of the maturity level of an existing information security management system based on ISO 21827
- Writing a business case and a project plan for the implementation of an ISMS
- Defining the scope of an ISMS
- Development of an ISMS and information security policies
- Selection of the approach and methodology for risk assessment
- Risk management: identification, analysis and treatment of risk (drawing on guidance from ISO/IEC 27005
- Drafting the Statement of Applicability
- Implementation of a document management framework
- Design of controls and writing procedures
- Implementation of controls
- Development of a training & awareness program and communicating about the information security
- Incident management (based on guidance from ISO 27035)
- Operations management of an ISMS

- Controlling and Monitoring the ISMS
- Development of metrics, performance indicators and dashboards in accordance with ISO 27004
- ISO/IEC 27001 internal Audit
- Management review of an ISMS
- Implementation of a continual improvement program
- Preparing for an ISO/IEC 27001 certification audit

INFOSECTRAIN

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

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

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

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 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

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

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

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

> 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

Section 27: Closing of the training course

> PECB certification scheme
> PECB certification process
> Other PECB services
> Other PECB training courses and certifications

www.infosectrain.com | sales@infosectrain.com