Table of Contents

Day 1 Introduction to ISO/IEC 27001 and initiation of an ISMS

- 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

Day 2 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

Day 3 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

Day 4 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