



ISO/IEC 27001 ISMS Implementation and Certification Readiness Course



ISO/IEC 27001 ISMS Implementation and Certification Readiness Course

Introduction:

ISO/IEC 27001 ISMS implementation and certification readiness is a 1-week course for information security, ISMS coordination, IT and risk staff, ending with an ISMS Implementation Plan and Mandatory Documented Information Set. Many organisations buy templates, rush the Statement of Applicability and reach the certification audit with an ISMS that exists on paper but has no working scope, risk method, audit programme or management review. Nominees already coordinate security, IT or risk work, and teaching is by case study on scopes, registers and records from several sectors. CoreConcept Training Center delivers this ISO/IEC 27001 ISMS implementation course.

Course Objectives:

- Determine the context, interested party requirements and ISMS scope required by clauses 4.1 to 4.3, including the climate change consideration added by Amendment 1:2024
- Draft an information security policy, assign leadership roles and set information security objectives with plans to achieve them
- Define a risk assessment and treatment methodology, then produce a risk treatment plan and a justified Statement of Applicability
- Establish competence, awareness, communication and documented information control arrangements that produce auditable records
- Set up monitoring and measurement, an internal audit programme, management review and a corrective action process
- Build an ISMS Implementation Plan and Mandatory Documented Information Set that shows readiness for certification

Target Audience:

- Information security managers accountable for establishing and running the ISMS
 - ISMS coordinators responsible for documented information, records and audit readiness
 - IT managers responsible for systems and services inside the ISMS scope
 - Risk managers responsible for the information security risk method and risk owners
 - Implementation team members responsible for project tasks and evidence collection
-

Course Outline:

Day 1: ISMS Foundations, Context and Gap Analysis

- Current ISO/IEC 27001 Edition, Amendment 1 and Harmonized Structure
- Clause 4.1 Internal, External and Climate Change Issues
- Clause 4.2 Interested Parties Requirements Register Construction
- Clause 4.3 ISMS Scope Boundaries, Interfaces and Dependencies
- Clauses 4 to 10 Gap Analysis Against Current Practice

Day 2: Leadership, Planning and the Risk Methodology

- Clause 5 Leadership Roles, Responsibilities and Authorities Assignment
- Clause 5.2 Information Security Policy Drafting and Approval
- Clause 6.1.2 Risk Assessment Methodology and Acceptance Criteria
- Clause 6.1.3 Risk Treatment Options and Plan Structure
- Clause 6.2 Information Security Objectives and Achievement Plans

Day 3: Support, Operation and Documented Information

- Annex A Comparison for the Statement of Applicability Decision
- Clause 7 Competence Records, Awareness Plans and Communication Matrix
- Clause 7 Documented Information Control and Version Management
- Clause 8 Operational Planning and Change Control Arrangements
- Clauses 8.2 and 8.3 Risk Assessment and Treatment Results Records

Day 4: Performance Evaluation, Improvement and Readiness Risks

- Clause 9 Monitoring and Measurement Method and Indicator Selection
- Clause 9 Internal Audit Programme Set-Up and Auditor Assignment
- Clause 9 Management Review Inputs, Outputs and Minutes
- Clause 10 Nonconformity, Corrective Action and Continual Improvement Log
- Certification Readiness Review of Common Documentation and Evidence Gaps

Day 5: Case Study Work and the ISMS Implementation Plan

- Case Study Scope and Context Analysis for a Logistics Provider
 - Case Study Risk Methodology and Statement of Applicability Defence
 - ISMS Implementation Project Plan with Milestones and Owners
 - Mandatory Documented Information Set Assembly and Peer Review
 - ISMS Implementation Plan and Documented Information Set Completion
-

Skills You Will Gain:

- ISMS Scope Definition
- Interested Party Analysis
- Risk Methodology Design
- Statement of Applicability Justification
- Documented Information Control
- Internal Audit Programme Planning
- Management Review Facilitation
- Implementation Project Planning

Why Attend This Course:

- Deliver an ISMS Implementation Plan and Mandatory Documented Information Set to the information security steering group and top management
- Decide which Annex A controls to include or exclude and record the justification in the Statement of Applicability
- Avoid certification audit delays caused by a missing scope, risk method, audit programme or management review record
- Brief risk owners, process owners and implementation team colleagues on the records each clause requires

Conclusion:

Back at work, the participant presents the ISMS Implementation Plan and Mandatory Documented Information Set to top management and the information security steering group. The organisation uses it to approve the ISMS scope, policy and risk method, assign owners and milestones, and decide when the system is ready for a certification body. After the first internal audit and management review under the plan, the team should review open nonconformities, missing records and slipped milestones and update the plan and document set.

Frequently Asked Questions FAQ:

What should participants know before an ISO/IEC 27001 ISMS implementation course?

No prior ISO/IEC 27001 training is required. Participants should already coordinate information security, IT or risk work, and bringing their organisation's current policies, risk register or scope notes helps apply the case study work to their own ISMS.

How does an ISO/IEC 27001 ISMS implementation course differ from a security controls course?

This course builds the management system itself through clauses 4 to 10: context, scope, leadership, risk method, support, operation, evaluation and improvement. A controls course concentrates on putting individual Annex A controls in place and testing them, which this course covers only for the Statement of Applicability decision.

Which documented information does an ISO/IEC 27001 ISMS implementation require?

The standard requires documented information including the ISMS scope, information security policy, risk assessment and treatment process, Statement of Applicability, risk treatment plan, objectives, risk results and evidence of competence, monitoring, internal audit, management review and corrective action.

What do participants take back from the ISO/IEC 27001 ISMS implementation course?

Participants take back an ISMS Implementation Plan with milestones and owners and a Mandatory Documented Information Set for their own scope, covering the policy, risk method, Statement of Applicability, objectives and the audit and review records the system must produce.
