+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 22/08/2025

Sign up

ISO/IEC 27001 Training - Information Security Management - Lead Auditor

ALL-IN-ONE: EXAM INCLUDED IN PRICE

5 days (35 hours)

PRESENTATION

The "ISO/IEC 27001 Lead Auditor - Information Security Management" course aims to give participants a solid understanding of the concepts and principles of an Information Security Management System (ISMS) based on the ISO/IEC 27001 standard. It covers the purpose of an ISMS, its structure, its links with other standards and its role in information security governance. This first step explains the conceptual framework and its significance in an audit context.

Trainees then learn how to interpret the requirements of ISO/IEC 27001 from an auditing perspective. Each clause is studied from a practical angle: scope identification, leadership, planning, governance, operational implementation and performance review. Emphasis is placed on the auditor's ability to relate normative requirements to organizational practices, and to understand how to assess compliance in the field.

A central part of the course is devoted to assessing the conformity of an ISMS. Participants discover how to assess the effectiveness of controls and measure the robustness of the system through documentary evidence, interviews and observations.
The approach is guided by the fundamental audit principles defined in ISO 19011, guaranteeing a professional, rigorous methodology in line with international best practice.

The course also covers all the steps required to plan, carry out and close an ISO/IEC 27001 audit. Trainees learn how to prepare an audit plan, conduct interviews, collect and analyze evidence, formulate and classify findings, write a clear report and present the results to management. Real-life situations are used to develop both the auditor's technical skills and posture.

At the end of the five-day course, participants will be able to conduct an end-to-end audit of

ISO/IEC 27001 compliance audit, in line with standards requirements and best auditing practices. They will have mastered the tools and methods needed to explain, interpret, evaluate and audit an ISMS effectively, and will be able to guarantee the value and credibility of their assignments to the organizations they audit.

Objectives

- Explain the concepts and principles of an ISMS based on ISO/IEC 27001
- Interpret the requirements of ISO/IEC 27001 in the context of an ISMS audit
- Assess the conformity of an ISMS to the requirements of ISO/IEC 27001 according to the fundamental concepts and principles of an audit
- Plan, carry out and close an audit of ISO/IEC 27001 compliance in accordance with auditing requirements and best practices

Target audience

- Project managers
- Consultants
- Technical architects
- Anyone wishing to conduct ISO/IEC 27001 compliance audits...

Prerequisites

- Know the basic principles of information security

Program of our ISO/IEC 27001 - Information Security Management - Lead Auditor training course

[Day 1 - Morning]

Key concepts of an ISMS

- Definitions: information asset, confidentiality-integrity-availability, stakeholders
- High-Level Structure of clauses 4 to 10 (2022)
- Relationship between ISO 27001 and ISO 27002, ISO 27005, ISO 31000
- Overview of SSI governance best practices
- Link between fundamental concepts and their role in a compliance audit
- Workshop: Mapping assets and visualizing priority data flows.

[Day 1 - Afternoon]

Principles and objectives of an ISO 27001 audit

- Differences between internal audit / third-party audit / certification
- ISO 19011 principles: ethics, fair presentation, risk-based approach
- Notions of compliance vs. effectiveness, types of evidence (documentary, observation, interview)
- Audit program life cycle: planning ? execution ? follow-up
- Comparison with the expectations of a certification auditor
- Workshop: Analyze a report extract to distinguish between findings, evidence and conclusions.

Interpret the requirements of clauses 4 and 5

- Organizational context & stakeholders
- Definition of scope and SSI policy
- Leadership, commitment and roles (Top Management, CISO, auditor)
- Document management and expected levels of proof
- Exercise in interpreting requirements in the role of auditor
- Workshop: Evaluating the relevance of an ISMS perimeter proposed by a customer.

[Day 2 - Morning]

ISMS planning (clause 6)

- Security objectives aligned with business strategy
- Risk assessment and treatment: ISO 27005 / EBIOS RM method
- Statement of Applicability: choice and justification of controls
- Action plans, resources and deadlines
- Audit approach: assessing the coherence and relevance of the SoA during an audit
- Workshop: Building a simplified SoA for a SaaS startup.

[Day 2 - Afternoon]

Support and governance (clause 7)

- Skills & security awareness (annual training plan)
- Internal / external communication, channels and responsibilities
- Documented information: policy, procedures, records, audit evidence
- Control of resources and supply chain
- Auditor's point of view: how to check documentary control and evidence
- Workshop: Analyze a document kit and detect critical gaps.

Interpreting Annex A 2022 (93 controls)

- New structure: 4 themes + attributes
- Organizational, human, technological and physical controls
- Focus on cloud & DevSecOps
- Risk-control link: prioritization & justification

- Audit application: verify implementation of controls through interviews and document reviews
- Workshop: Selecting 20 controls for a multicloud environment.

[Day 3 - Morning]

Operational functioning (clause 8)

- Operating processes: change, backup, logging, access
- Incident management: detection, response, learning
- Risk acceptance criteria & residual treatment
- Legal / forensic evidence requirements
- Auditor positioning: what evidence to look for to assess operational compliance.
- Workshop: "ransomware incident" role-playing game and evidence gathering.

[Day 3 - Afternoon]

Assessing ISMS compliance and performance (clause 9)

- KPI/KRI indicators, ISMS dashboards
- Evaluating the effectiveness of measures in relation to standard requirements
- Internal audit: objectives, scope, criteria, methods
- Management review: mandatory inputs/outputs
- Stakeholder satisfaction & participative improvement
- Cross-audit situation between trainees (auditors/audited)
- Workshop: Defining three relevant indicators for a hospital.

Continuous improvement (clause 10)

- Non-conformities, corrective actions (CAPA) and improvement loops
- Capitalizing on incidents and feedback
- Integration with other management systems (ISO 9001, 22301)
- Safety culture: advanced awareness programs
- Analysis of an audit case with real non-conformities and CAPA proposal
- Workshop: Building a CAPA plan based on fictitious audit findings.

[Day 4 - Morning]

Detailed audit plan and logistical preparation

- Define objectives, scope, criteria, methods
- Team allocation: skills, independence, man-days
- Checklist & interview guides based on ISO 27001
- Engagement letter, communication with the auditee, preliminary document management
- Workshop: Setting up an audit schedule for two remote sites.

[Day 4 - Afternoon]

Evidence gathering techniques

- Observation, interviews, document review, technical tests
- Sampling and representativeness
- Time management and on-site adaptation
- Digital tools: remote auditing, secure recording of evidence
- Workshop: Simulation of an auditor-audited interview on access management.

Analysis of findings and report writing

- Classification: major / minor non-conformity, opportunities for improvement
- SMART formulation and traceability of evidence
- Structure of the ISO 27001 report for a certification body
- Closing meeting: assertive communication techniques
- Case study: oral presentation of audit results to a fictitious board of directors
- Workshop: Writing the executive summary in 15 minutes.

[Day 5 - Morning]

ISO 27001 certification process

- Stages: application review, Stage 1, Stage 2, surveillance audits, recertification
- Accreditation criteria and role of the certification body
- Post-audit deviation management and follow-up
- Multi-site strategies & sampling
- Workshop: Planning the certification roadmap for a European SME.

[Day 5 - Afternoon]

Consulting and support for organizations

- Positioning the Lead Auditor / consultant role
- Value argument and return on security investment
- Change management and ISMS project management
- Aligning ISO 27001 with NIS 2, DORA, NIST CSF frameworks
- Workshop: Building an "ISO 27001 ROI" consulting pitch for senior management.

Final exam preparation

- Standard exam structure
- Time management techniques and avoiding pitfalls

- Administrative tips: registration, identification, remote monitoring
- Pedagogical workshop: Practice exam and correction.

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.