Publication date : 03/05/2025

Course : Lead Auditor - ISO 27001:2022 certification LSTI

Implementing and managing an ISO 27001:2022 project

Practical course - 5d - 35h00 - Ref. PIS

Price : 3430 € E.T.

BEST

The ISO/CEI 27001 international standard for information security risk management describes, in the form of requirements, the best practices to be put in place so that an organization can effectively manage information-related risks. This seminar will first introduce you to all the ISO standards dealing with information system security, and then provide you with the elements you need to set up an information security risk management system (ISMS).

Teaching objectives

At the end of the training, the participant will be able to:

- Explain the components of an ISO 27001-compliant information security management system (ISMS)
- Adapt ISO 27001 requirements to an organization's specific context
- Prepare for and take the [[Lead Auditor 27001:2022]" exam

Intended audience

CISOs, risk managers, IT directors or managers, project managers, security engineers or correspondents, project managers, internal and external auditors, future "auditees".

Prerequisites

Basic knowledge of IT security.

Certification

To take this exam remotely, the candidate must acquire all the necessary standards in paper format. End-of-session certification exam in French. This exam certifies that you have the knowledge and skills required to audit the conformity of an ISMS to the ISO/IEC 27001:2022 standard. This exam is run in partnership with the certification body LSTI.

Remote certifications

See the certifier's official documentation for the list of prerequisites for completing the online certification exam.

PARTICIPANTS

CISOs, risk managers, IT directors or managers, project managers, security engineers or correspondents, project managers, internal and external auditors, future "auditees".

PREREQUISITES

Basic knowledge of IT security.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

Practical details

Hands-on work

Preparation for ISO 27001 Lead Implementer and Lead Auditor certification.

Composition de la formation

Implement and manage an ISO 27001:2013 Project

Ref. ASE - 3 days ★ 4 / 5

ISO 27001:2013 Lead Auditor, Certification

Ref. LAU - 2 days

Course schedule

1 Introduction

- Reminders. ISO 27000 and ISO Guide 73 terminology.
- Definitions: threat, vulnerability, protection.
- The notion of risk (consequence, impact, likelihood).
- Minimum CID classification (Confidentiality, Integrity, Availability).
- Risk management (reduction, maintenance, refusal, sharing).
- Claims analysis. Trends. Challenges.
- Security regulations (business, legal...) PCI-DSS, NIST, LPM/NIS. Who is it for? For whom? Interaction with ISO.
- ISO alignment with Governance / Protection / Defense / Resilience.

2 ISO 2700x standards

- History of ISO safety standards.
- BS 7799 standards, their contribution to ISO.
- Current standards (ISO 27001, 27002).
- Complementary standards (ISO 27005, 27004, 27003, etc.).
- Convergence with 9001 quality and 14001 environmental standards.
- The contribution of qualiticians to safety.

3 The ISO 27001:2022 standard

- Definition of an ISMS.
- Objectives to be achieved by your ISMS.
- The "continuous improvement" approach as a founding principle, the PDCA model (Deming wheel).
- ISO 27001 integrated into a global approach to ISS governance.
- Details of Plan-Do-Check-Act phases.
- From ISMS perimeter specification to SoA (Statement of Applicability).
- ISO 27001 recommendations for risk management.
- The importance of risk assessment. Choosing a method such as ISO 27005:2022 / ISO 31000.
- The contribution of published methods (e.g. EBIOS) to their assessment process.
- The adoption of efficient technical and organizational security measures.
- Mandatory internal ISMS audits. Building an audit program.
- ISMS improvement. Implementation of corrective and preventive actions.
- Appendix A as a reference tool - link with standard 27002.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

4 Best practices, ISO 27002:2022 standard

- First-level structuring: organizational, personal, physical and technological measures.
- Themes and attributes (#Prevention, #Detection, #Correction).
- Cybersecurity concepts (#Identification, #Protection, #Detection, #Processing, #Recovery).
- Operational capabilities (#Governance, #Asset_Management, Information_Protection...).
- Safety domains ((#Governance_and_ecosystem, #Protection, #Defense, #Resilience).
- ISO 27002:2022: an overview of 93 best practices.
- New ISO 27002:2022 best practices, measures removed from ISO 27001:2017. Modifications.
- Examples of how to apply the new standard to your organization: key security measures.

5 Safety audits: ISO 19011:2018 and ISO 17021:2015 standards

- Continuous, comprehensive process. Stages, priorities.
- Building an internal audit program.
- Audit categories: organizational, technical...
- Internal, external and third-party audits.
- Typical ISO audit procedure, key stages.
- Audit objectives, audit quality.
- The improvement approach to auditing.
- Auditor qualities and assessment.
- Auditing management system governance: approach and methods.

6 ISO certification of IS security: the ISMS certificate

- What's interesting about this approach is the search for the "label".
- Criteria for selecting the perimeter. Scope of application. Involvement of interested parties.
- ISO: an essential complement to regulatory frameworks and standards?
- Expected business and/or regulatory challenges.
- Certifying bodies, selection in France and worldwide.
- Audit process, stages and workloads.
- ISO 17021 and ISO 27006 standards, obligations for certifiers.
- Certification costs, ROI.

7 Preparing for and taking the exam

- Necessary standards: ISO 27000, ISO 27001, ISO 27002, ISO 27005, ISO 19011, ISO 17021, ISO 27006.
- On the first day of training, we'll explain the content and rules of the online exam.
- Technical requirements for online testing (webcam enabled, Internet connection).
- This exam takes place on the TESTWE online exam platform (testwe.eu).
- If the exam is taken on Orsys premises, Orsys will take care of preparing the candidate's workstation.
- When you take the exam at Orsys, you will also receive a paper copy of the standards described during the training course.
- To take the exam remotely, candidates must acquire all the standards themselves in paper format.

Exam

The exam consists of a multiple-choice/question-and-answer format. It lasts 2h30. It is worth 100 points. If at least 65% of answers are correct, the exam is passed.

Dates and locations

REMOTE CLASS
2026 : 27 May, 22 June, 29 June, 28 Sep., 5 Oct., 9 Nov., 30 Nov., 7 Dec.

PARIS LA DÉFENSE
2026 : 18 May, 22 June, 28 Sep., 2 Nov., 30 Nov.