+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

Training ISO/IEC 27001 - Information Security Management - Foundation

ALL-IN-ONE : EXAM INCLUDED IN PRICE

2 days (14 hours)

PRESENTATION

Our "ISO/IEC 27001 Foundation" training course provides a proven framework for protecting your critical assets, gaining your customers' trust and meeting regulatory requirements (RGPD, NIS 2...). Based on the latest version 2022, ISO/IEC 27001 is the international reference standard for building, managing and upgrading an Information Security Management System (ISMS).

This immersive training course provides you with everything you need to understand, deploy and audit an ISMS effectively: decoding the standard, analyzing in detail applicable clauses 4 to 10 of ISO/IEC 27001 and the new HLS structure, as well as Annex A and its 93 controls.

We will also look at other related standards, in particular ISO/IEC 27002, which complements 27001 with detailed recommendations for implementing security controls. The focus will be on the new features of version 2022: cloud cybersecurity, threat intelligence, digital continuity, supplier governance, etc.

At the end of this course, you'll have mastered the fundamentals of the ISO/IEC 27001 standard for implementing an ISMS.

Like all our training courses, this one favors a practical and operational approach, with workshops, case studies and a mock exam to prepare effectively for ISO/IEC 27001 Foundation certification.

OBJECTIVES

- Understand how an ISMS works

- Understand the ISO 27001 and ISO 27002 standards
- Know the methods and techniques for implementing and managing an ISMS.

TARGET AUDIENCE

- Anyone involved in information security management or wishing to acquire knowledge of the main processes of an information security management system and/or pursue a career in information security management.

Prerequisites

- This course has no prerequisites

Our ISO 27001 Foundation training program

[Day 1 - Morning]

Introduction to ISO/IEC 27001 and ISMS

- Understanding ISO/IEC 27001 and its role in cybersecurity
- Clauses 1 to 3: introductory (purpose, references, definitions)Clauses 4 to 10: ISMS certification requirements (context for improvement)
- Definition of an ISMS and organizational issues
- Relationship with other standards, in particular ISO/IEC 27002 for security measures (best practices and implementation of controls)
- Overview of related standards: ISO/IEC 27005 (risk management), ISO/IEC 27035 (incidents)
- Practical workshop: Identifying risks in a fictitious organization.

[Day 1 - Afternoon]

Context, leadership and ISMS planning

- Context analysis and stakeholders
- Management commitment and key roles
- Risk management and security planning (PDCA approach and continuous improvement cycle)
- Practical workshop: Drawing up a simplified security policy.

Support, operations and performance

- Resources and skills management
- Awareness, communication and documentation
- Performance assessment and internal audits
- Practical workshop: Building a security awareness plan.

[Day 2 - Morning]

Security measures and ISO 27001 annexes

- Presentation of ISO 27001 Annex A and its 93 controls
- Correspondence with ISO 27002: practical recommendations and examples
- Highlighting the new features of version 2022: cloud, threat intelligence, supplier governance, etc.
- Organizational security, access control, communications protection
- Practical workshop: Study scenarios and propose controls.

[Day 2 - Afternoon]

Compliance, improvement and certification

- ISO 27001 compliance audits
- Corrective actions and continuous improvement (approach based on risk analysis and performance indicators)
- Certification process and preparation
- Practical workshop: Performing an ISO 27001 self-assessment.

Preparing for the ISO 27001 Foundation exam

- Exam format, duration and requirements
- Tips and strategies for success
- Simulated exam questions
- Practical workshop: Taking and marking a mock exam.

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 enrolment is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level in different types of technology, as well as his or her expectations and objectives.

This questionnaire also enables us to anticipate any connection or internal security problems (intra-company or virtual classroom) that could be problematic for the follow-up and smooth running of the training session. This questionnaire also enables us to anticipate any connection or internal security difficulties within the company (intra-company or virtual classroom) that 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.