+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 27005 Certification Training -Risk Manager

ALL-IN-ONE: EXAM INCLUDED IN PRICE

3 days (21 hours)

Presentation

Our "ISO/IEC 27005 - Risk Manager" course provides participants with a clear understanding of the essential concepts of information security risk management, as defined by the ISO/IEC 27005 standard.

It teaches how to interpret the requirements of ISO/IEC 27001 and effectively integrate risk management into an Information Security Management System (ISMS).

Through case studies and workshops, trainees develop the skills needed to identify, assess and deal with risks, by constructing relevant scenarios and drawing up appropriate treatment plans.

Particular emphasis is placed on operational implementation: definition of security measures, preparation of the risk treatment plan (PTRA) and reporting to decision-making bodies.

At the end of the course, participants will be able to pilot a risk management approach in line with international standards, and to capitalize on their experience by preparing for ISO/IEC 27005 Risk Manager certification.

Objectives

- Understand the key concepts of risk management as defined by the ISO/IEC 27005 standard.

- Interpret risk management requirements within an ISO/IEC 27001-compliant ISMS
- Identify, assess and address information security risks

Target audience

- CISOS
- Project managers
- Consultants
- Anyone in charge of information security, compliance and risk management in an organization

Prerequisites

- Basic knowledge of risk management and information systems security.

Our ISO/IEC 27005 - Risk Manager Training Program

[Day 1 - Morning]

Introduction to risk management in information security

- Risk definition and C/I/D issues (confidentiality, integrity, availability)
- Overview of current threats (cyber-attacks, malware, human error, etc.) and vulnerabilities
- Introduction to ISO/IEC 27005 and other key risk management standards
- Presentation of key risk management norms and standards
- The Risk Manager's role in the ISMS for identifying and dealing with risks
- Practical workshop: Identification of known risks in the company.

[Day 1 - Afternoon]

Fundamental concepts and standards in risk management

- Terminology: asset, threat, vulnerability, impact, probability
- Importance of risk management in an ISMS and link with compliance
- Frameworks and methods: ISO/IEC 27005, EBIOS, MEHARI, NIST RMF - articulation
- Critical comparison of approaches (strengths/weaknesses) to position ISO/IEC 27005 as the linchpin of an ISMS
- Risk governance: global process and integration with corporate strategy
- Practical workshop: Quiz/validation of definitions & associated standards.

ISO/IEC 27005 process (Part 1) - Contextualization & risk identification

- Setting the context: scope, critical assets, business challenges, acceptance criteria
- Identification and valuation of information assets (data, infrastructure, applications)
- Identification of threats and vulnerabilities by asset
- Risk scenarios: combination of assets/threats/vulnerabilities and initial impact estimates
- Direct link with ISO/IEC 27001 requirements (e.g. §6.1.2 on the identification and treatment of information security risks)
- Practical workshop: Defining the scope and carrying out initial risk mapping.

[Day 2 - Morning]

ISO/IEC 27005 process (Part 2) - Risk analysis & assessment

- Analysis: likelihood & impact estimation for each scenario
- Estimation methods: quantitative vs. qualitative approaches
- Evaluation/prioritization: probability/impact matrix and identification of unacceptable risks
- Risk appetite and tolerance: acceptability decisions
- Putting into perspective the role of leadership (ISO 27001 §5.1) in validating risk appetite
- Practical workshop: Estimating impacts & probabilities and positioning on the matrix.

[Day 2 - Afternoon]

Integrating risk management into ISO/IEC 27001

- ISO/IEC 27005 link ? ISO/IEC 27001: risk management as the foundation of the ISMS
- Selection/justification of measures via Annex A (ISO 27001:2022)
- Drawing up a risk treatment plan (PTRA): prioritization, responsibilities, resources
- Residual risk monitoring and validation by management
- Communication & reporting (reports, dashboards) to stakeholders
- Continuous improvement in the PDCA cycle
- Operational translation of measures into appropriate SSI policies and procedures (e.g. access management, backup, data classification).
- Collective feedback and sharing of identified best practices.
- Practical workshop: Building an ISO 27001 PTRA extract + reporting to COMEX.

[Day 3 - Morning]

Global risk management case study

- End-to-end application of the ISO/IEC 27005 process to a complex scenario

- Risk mapping, estimation, analysis and treatment plan
- Presentation & justification of trade-offs before a mock jury
- Practical workshop: Team presentation of mapping and treatment plan.

[Day 3 - Afternoon]

Best practices, success factors & feedback

- Management involvement, clear scope, up-to-date risk register
- Common mistakes & pitfalls to avoid
- Governance: roles of risk committee, risk owner, SSI correspondents
- GRC tools, ANSSI resources, knowledge bases and specialized software
- Complementary module: regulatory watch and compliance (RGPD, NIS2, DORA) to contextualize risk management in the legal and sectoral environment
- Practical workshop: experience sharing & benchmarking led by the trainer.

Preparation for ISO/IEC 27005 Risk Manager certification

- Exam format: MCQ, duration, pass score, language
- Tips for success: time management, reading techniques
- Review of key points (standards, processes, risk calculations, etc.)
- Q/R session & memorization tips
- Practical workshop: mock 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 IT 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 and

and group work sessions.

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.