



Training sheet
ISO 27005 – Risk Manager
certification

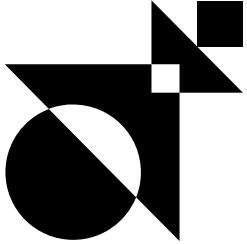
CONTACT FOR THIS TRAINING

Miora RAHARINIRINA
Almond Institute coordinator
almond.institute@almond.eu
07 64 42 71 56

→ Version 1.0

→ 08/12/2023

Course overview



This course provides participants with the skills to master the basic elements of information security risk management using ISO/IEC 27005 as a framework. Through practical exercises and case studies, participants will acquire the skills and competencies necessary to perform an optimal information security risk assessment and manage risk over time by being familiar with their lifecycle. This training fits perfectly into the ISO/IEC 27001 implementation process.

01 ■

Understand the concepts, approaches, methods and techniques for **effective risk management in ISO 27005**

03 ■

Acquire the skills to **implement, maintain and manage an ongoing information security risk management program**

02 ■

Interpret the risk management requirements of ISO 27001 to **understand the relationship between an information security management system, security measures, and compliance** with the requirements of an organization's various stakeholders

04 ■

Acquire the skills to **effectively advise an organization** on best practices in information security risk management

Useful informations

Who should attend?

- Risk Managers
- Individuals responsible for information security or compliance within an organization
- Member of an information security team
- Information technology consultants
- Personnel implementing or seeking compliance with ISO 27001 or participating in a risk management program

Entry requirements

- General knowledge of information systems
- General knowledge of information systems security
- General knowledge of risk management

Method of assessment

The "PECB Certified ISO/IEC 27005 Risk Manager" exam lasts 2 hours.
The exam covers the following areas:

- Domain 1: Fundamental principles and concepts, methods and techniques of risk management
- Domain 2: Implementation of a risk management program
- Domain 3: Risk analysis in information security according to ISO 27005

How and when to access

The participant is considered registered when:

- The prerequisites and needs are identified and validated
- The training agreement is signed

Registration requests can be sent up to 10 working days before the start of the training.

To go further

This training course is a preparation for the following training course:

- EBIOS Risk Manager certification

Accessibility

Whether you are recognized as having a disability or not, making our training accessible to everyone is part of our commitment. If you need compensation or adaptation for the content, the supports, the "venue", the material used, the schedules, the rhythm, **we are at your disposal.**

Face-to-face training

Course curriculum

Day 1	Day 2	Day 3
Introduction, risk management program, risk identification and analysis according to ISO 27005	Risk assessment, treatment, acceptance according to ISO 27005	Cross-functional risk management and other methodologies
<ul style="list-style-type: none">→ Concepts and definitions related to risk management→ Risk management standards, frameworks and methodologies→ Implementation of a risk management program in information security→ Risk analysis (Identification and estimation)	<ul style="list-style-type: none">→ Risk Assessment→ Risk treatment→ Risk acceptance in information security and residual risk management	<ul style="list-style-type: none">→ Risk Communication in Information Security→ Risk monitoring and control in information security→ Overview of existing methodologies (including Ebios)→ Assessment and review

Training benefits

This training is based on alternating theoretical and practical sessions:

- Lectures illustrated with examples from real cases
- Classroom exercises to help prepare for the exam
- Practical tests similar to the certification exam

In order to preserve the good realization of the practical exercises, the number of participants in the training is limited.

Price and informations



- **Duration:** 3 days (19 hours)
- **Meal:** breakfast and meal included
- **Price:** 2300€ escl. tax.
- **Financing:** OPCO support

Distance learning

Course curriculum

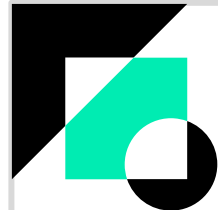
→ 14h distance learning with the trainer

Session 1	Session 2	Session 3	Session 4
<ul style="list-style-type: none"> → Section 1: Training objectives and structure → Section 2: Standards and regulations 	<ul style="list-style-type: none"> → Section 3: Risk concepts and definitions → Section 4: Risk management program 	<ul style="list-style-type: none"> → Section 5: Setting the context 	<ul style="list-style-type: none"> → Section 6: Risk identification → Section 7: Risk analysis
Session 5	Session 6	Session 7	Session 8
<ul style="list-style-type: none"> → Section 8: Risk assessment → Section 9: Risk assessment using a quantitative method → Section 10: Risk treatment 	<ul style="list-style-type: none"> → Section 11: Acceptance of information security risks → Section 12: Communication and consultation on information security risks 	<ul style="list-style-type: none"> → Section 13: Information security risk monitoring and review / Section 14: OCTAVE Method / Section 15: MEHARI Method / Section 16: EBIOS Method / Section 17: Harmonized threat and risk assessment (TRA) method / Section 18: Certification process and end of training course 	<ul style="list-style-type: none"> → Revisions

Training benefit

- Training by a cybersecurity expert
- An intuitive, easy-to-use platform
- Exchanges on key concepts and experience sharing adapted to the learners' context
- Training methods adapted to all learning profiles
- The structure of the questionnaires is similar to that of the certification exam

Price and informations



- **Duration:** 21 hours
- **Price:** 1950€ excl. tax.
- **Financing:** OPCO support