ISO 27005 – Risk Manager Certification

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.

1 On-site training

Overview

- Understand the concepts, approaches, methods and techniques for effective risk management in ISO 27005
- Interpret the risk management requirements of ISO 27001 to understand the relationship between an information security management system, security measures and compliance with requirements of organization multiple stakeholders
- Acquire the skills to implement, maintain and manage an ongoing information security risk management program
- Acquire the skills to effectively advise an organization on best practices in information security risk management

Course Curriculum

Day 1: Introduction, risk management program, risk identification and analysis according to ISO 27005

- Risk Management concepts and definitions
- Standards, frameworks and methodologies in risk management
- Implement a risk management program in information security
- Risk analysis (Identification and assessment).

Day 2: Risk assessment, treatment, acceptance according to ISO 27005

- Risk assessment
- Risk treatment
- Risk acceptance in information security and residual risk management

Day 3: Transversal functions of risk management and other methodologies

- Risk communication in information security
- Monitoring and control of risk in information security
- Overview of existing methodologies (including Ebios)
- Assessment and review

Learning Assessment

The "PECB Certified ISO/IEC 27005 Risk Manager" exam is held on the 3rd day of training and lasts 2 hours. The exam covers the following areas:

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

Practical information

Duration: 3 days (24 hours)

Price: €2000€ excl tax

CPF / OPCO support

Breakfast & lunch included

The +

This training is based on the alternation of theoretical and practical time:

- Lecture illustrated with examples from real cases
- In-class 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.

Who should attend?

- Risk managers
- Any individual responsible for information security or compliance within an organization
- Member of an information security team
- IT consultants
- Any individual implementing ISO/IEC 27001, wanting to comply with ISO/IEC 27001 or involved in a risk management program.

Prerequisites

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

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 5 working days before the start of the training.

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 place, the material used, the schedules, the rhythm, we are at your disposal.

2 Distance learning training

Overview

- Understand the concepts, approaches, methods and techniques for effective risk management in ISO 27005
- Interpret the risk management requirements of ISO 27001 to understand the relationship between an information security management system, security measures and compliance with requirements of organization multiple stakeholders
- Acquire the skills to implement, maintain and manage an ongoing information security risk management program
- Acquire the skills to effectively advise an organization on best practices in information security risk management

Course Curriculum

Session 1: Key concepts

- The ISO model
- The normative framework
- Definition of risk

Session 2: Establishing the context

- The objectives of risk management
- The influences of objectives and context on the risk management process
- Getting ready

Session 3: Risk management approach and criteria

- Choice of methodology
- Definition of risk criteria
- Construction of rating scales

Session 4: Risk evaluation

- Risk identification
- Risk analysis
- Risk assessment

Session 5: Risks treatment

- Decision-making
- Risk treatment choices
  The risk treatment plan

Session 6: Cross-functional risk management processes

- When and what to communicate
- Making decisions
- Revision

Principle planning

- 12 hours of classes with the trainer divided into 5 sessions of 1h30 to 2h
- 10 hours of personal work time in autonomy

	Monday	Tuesday	Wednesday	Thursday	Friday
Week 1	Introduction		Session 1	Session 2	Session 3
Week 2	Session 4	Session 5	Session 6	Revision	Exam

Learning assessment

- 2H closed book distance exam
- Consists of a total of 100 multiple choice questions

Practical informations

Duration: 24 hours

Price: €1800 excl tax

CPF/OPCPO support

The +

- Training provided by a cybersecurity expert
- An intuitive and easy-to-use platform
- Exchange moments on key concepts and experience sharing adapted to the learners' context
- A training pedagogy adapted to all learning profiles

Who should attend?

- Information Security Managers
- Information Security Team Members

- Any individual responsible for information security, compliance and risk in an organization
- Any individual implementing ISO/IEC 27001, wanting to comply with ISO/IEC 27001 or involved in a risk management program
- IT consultants
- IT professionals
- Information Security Officers
- Data Protection Officers

Prerequisites

A fundamental understanding of ISO/IEC 27005 and a thorough knowledge of risk assessment and information security.

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 5 working days before the start of the training.

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 place, the material used, the schedules, the rhythm, we are at your disposal.