ISO 27005 Risk Manager

⌖ **E-Learning**
Online instructor-led
Self-study
Modality

⌖ **English**
Spanish
Language

🕐 **3 days**
Duration

Gain the essential skills to implement and support an information security risk management programme with the ISO/IEC 27005:2022 Risk Manager course. In just 3 days, you'll learn how to identify, assess, treat, and communicate risks in alignment with ISO/IEC 27005 and ISO 31000, while supporting broader compliance with ISO/IEC 27001.

This course combines theory with practical exercises, quizzes, and case studies. You'll also explore well-established risk assessment methodologies such as OCTAVE, MEHARI, EBIOS, NIST, CRAMM, and TRA. Upon passing the exam, you can apply for the PECB Certified ISO/IEC 27005:2022 Risk Manager credential — a valuable proof of your competency in the field of IS risk.

Learning Objectives

By the end of the course, you will be able to:

✓ Explain key risk management concepts under ISO/IEC 27005:2022 and ISO 31000

✓ Establish, maintain and improve an information security risk management framework based ISO 27005

⊘ Apply risk assessment, treatment, and communication processes

⊘ Understand and leverage multiple risk methodologies (OCTAVE, MEHARI, NIST, etc.)

Who Should Attend?

🔍 Managers and consultants involved in information security

⊗ IT professionals and privacy officers

✓ Project managers or expert advisers seeking to master the management of information security risks

▭ Individuals responsible for maintaining conformity with ISO/IEC 27001

▭ Individuals responsible for managing information security risks

What's Included?

▭ 350+ pages of training material, practical cases, and exercises

▤ Certification and exam fees

⊘ Course completion attestation, granting 21 CPD credits.

Course Agenda

Day 1 | Introduction to ISO/IEC 27005:2022 and risk management

- Training course objectives and structure
- Standards and regulatory frameworks
- Fundamental concepts and principles of information security risk management

- Information security risk management program
- Context establishment

Day 2 Risk assessment, risk treatment, and risk communication and consultation based on ISO/IEC 27005:2022

- Risk identification
- Risk analysis
- Risk evaluation

- Risk treatment
- Information security risk communication   and consultatio

Day 3 Risk recording and reporting, monitoring and review, and risk assessment method

- Information security risk recording and reporting
- Information security risk monitoring and review
- OCTAVE and MEHARI methodologies

- EBIOS method and NIST framework
- CRAMM and TRA methods
- Closing of the training course

Certification & Exam

🎓 Certification Prerequisites

After successfully completing the exam, you can apply for one of the credentials shown on the table below. You will receive a certificate once you meet the requirements related to the selected credential.

	ISO/IEC 27005:2022 Provisional Risk Manager	ISO/IEC 27005:2022 Risk Manager	ISO/IEC 27005:2022 Senior Risk Manager	Other requirements
General Work Experience	None	2 Years	10 Years	
Information Security Management experience	None	1 year	7 Years	Signing the PECB Code of Ethics
Hours of Information Security Risk Management activities	None	200 hours	1000 hours	

📄 **Exam:** 2 hours, taken on Day 3

It covers the following competency domains:

Domain 1 | Fundamental principles and concepts of information security risk management.

Domain 2 | Implementation of an information security risk management program.

Domain 3 | Information security risk management framework and processes based on ISO/IEC 27005:2022.

Domain 4 | Other information security risk assessment methods.

⊘ **Retake:** Free retake within 12 months if needed

📄 **Maintenance Fee:** First year included; fees applies from second year. Pay $120/year or save 10% by paying three years upfront.