PECB Certified ISO/IEC 27005
Lead Risk Manager

Master the fundamental principles and concepts of Risk Assessment and Optimal Risk Management in Information Security based on ISO/IEC 27005

Why should you attend?

ISO/IEC 27005 Lead Risk Manager training enables you to develop the competence to master the risk management process related to all assets of relevance for Information Security using the ISO/IEC 27005 standard as a reference framework. During this training course, you will gain a comprehensive knowledge of a process model for designing and developing an Information Security Risk Management program. The training will also contain a thorough understanding of best practices of risk assessment methods such as OCTAVE, EBIOS, MEHARI and harmonized TRA. This training course supports the implementation process of the ISMS framework presented in the ISO/IEC 27001 standard.

After mastering all the necessary concepts of Information Security Risk Management based on ISO/IEC 27005, you can sit for the exam and apply for a "PECB Certified ISO/IEC 27005 Lead Risk Manager" credential. By holding a PECB Lead Risk Manager Certificate, you will be able to demonstrate that you have the practical knowledge and professional capabilities to support and lead a team in managing Information Security Risks.

Who should attend?

- Information Security risk managers
- Information Security team members
- Individuals responsible for Information Security, compliance, and risk within an organization
- Individuals implementing ISO/IEC 27001, seeking to comply with ISO/IEC 27001 or individuals who are involved in a risk management program
- IT consultants
- IT professionals
- Information Security officers
- Privacy officers

Course agenda

Duration: 5 days

Day 1 | Introduction to ISO 27005, concepts and implementation of a risk management program

- Course objectives and structure
- Standard and regulatory framework
- Concepts and definitions of risk
- Implementing a risk management programme
- Context establishment

Day 2 | Risk identification, evaluation, and treatment as specified in ISO 27005

- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Assessment with a quantitative method
- Risk Treatment

Day 3 | Information Security Risk Acceptance, Communication, Consultation, Monitoring and Review

- Information security risk acceptance
- Information security risk communication and consultation
- Information security risk monitoring and review

Day 4 | Risk Assessment Methodologies

- OCTAVE Method
- MEHARI Method
- EBIOS Method
- Harmonized Threat and Risk Assessment (TRA) Method
- Applying for certification and closing the training

Day 5 | Certification Exam

Learning objectives

- Understand the concepts, approaches, methods and techniques that enable an effective risk management process according to ISO/IEC 27005
- Acknowledge the correlation between Information Security risk management and security controls
- Learn how to interpret the requirements of ISO/IEC 27001 in Information Security Risk Management
- Acquire the competence and skills to effectively advise organizations on Information Security Risk Management best practices
- Acquire the knowledge necessary for the implementation, management and maintenance of an ongoing risk management program

Examination

Duration: 3 hours

The "PECB Certified ISO/IEC 27005 Lead Risk Manager" exam fully meets the requirements of the PECB Examination and Certification Programme (ECP). The exam 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 assessment

Domain 4 | Information security risk treatment

Domain 5 | Information security risk communication, monitoring and improvement

Domain 6 | Information security risk assessment methodologies

For more information about exam details, please visit Examination Rules and Policies.

Certification

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

For more information about ISO/IEC 27005 certifications and the PECB certification process, please refer to the Certification Rules and Policies.

Credential	Exam	Professional experience	Information Security Risk Management experience	Other requirements
PECB Certified ISO/IEC 27005 Provisional Risk Manager	PECB Certified ISO/IEC 27005 Risk Manager exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27005 Risk Manager	PECB Certified ISO/IEC 27005 Risk Manager exam or equivalent	**Two years:** One year of work experience in ISRM	Information Security Risk Management activities: a total of 200 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27005 Lead Risk Manager	PECB Certified ISO/IEC 27005 Lead Risk Manager exam or equivalent	**Five years:** Two years of work experience in ISRM	Information Security Risk Management activities: a total of 300 hours	Signing the PECB Code of Ethics

General information

- Certification fees are included on the exam price
- Training material containing over 350 pages of information and practical examples will be distributed
- A participation certificate of 21 CPD (Continuing Professional Development) credits will be issued
- In case of exam failure, you can retake the exam within 12 months for free