PECB Certified ISO/IEC 27005
Lead Risk Manager

Obtain the necessary knowledge and competencies to support organizations establish information security risk management frameworks based on ISO/IEC 27005 and other risk assessment methodologies

Why should you attend?

Risk management is an essential component of any information security program. An effective information security risk management program enables organizations to detect, address, mitigate, and even prevent information security risks.

The ISO/IEC 27005 Lead Risk Manager training course provides an information security risk management framework based on ISO/IEC 27005 guidelines, which also supports the general concepts of ISO/IEC 27001. The training course also provides participants with a thorough understanding of other best risk management frameworks and methodologies, such as OCTAVE, EBIOS, MEHARI, CRAMM, NIST, and Harmonized TRA.

The PECB ISO/IEC 27005 Lead Risk Manager certificate demonstrates the individual has acquired the necessary skills and knowledge to successfully perform the processes needed for effectively managing information security risks. It also proves that the individual is able to assist organizations in maintaining and continually improving their information security risk management program.

The training course is followed by an exam. If you pass, you can apply for a "PECB Certified ISO/IEC 27005 Lead Risk Manager" credential. For more information about the examination process, please refer to the Examination, Certification, and General Information section below.

Who should attend?

This training course is intended for:

- Managers or consultants involved in or responsible for information security in an organization
- Individuals responsible for managing information security risks, such as ISMS professionals and risk owners
- Members of information security teams, IT professionals, and privacy officers
- Individuals responsible for maintaining conformity with the information security requirements of ISO/IEC 27001 in an organization
- Project managers, consultants, or expert advisers seeking to master the management of information security risks

Course agenda

Duration: 5 days

Day 1 | Introduction to ISO/IEC 27005 and information security 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 identification, analysis, evaluation, and treatment based on ISO/IEC 27005

- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment

Day 3 | Information security risk communication and consultation, recording and reporting, and monitoring and review

- Information security risk communication and consultation
- Information security risk recording and reporting
- Information security risk monitoring and review

Day 4 | Risk assessment methods

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

Day 5 | Certification Exam

Learning objectives

By successfully completing this training course, you will be able to:

- Explain the risk management concepts and principles based on ISO/IEC 27005 and ISO 31000
- Establish, maintain, and continually improve an information security risk management framework based on the guidelines of ISO/IEC 27005 and best practices
- Apply information security risk management processes based on the guidelines of ISO/IEC 27005
- Plan and establish risk communication and consultation activities
- Record, report, monitor, and review the information security risk management process and framework

Examination

Duration: 3 hours

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

Domain 4 | Information security risk treatment

Domain 5 | Information security risk communication, monitoring, and improvement

Domain 6 | Information security risk assessment methodologies

For specific information about the exam type, languages available, and other details, please visit the List of PECB Exams and Exam Rules and Policies.

Certification

Upon the successful completion of the exam, you can apply for the "PECB Certified ISO/IEC 27005 Lead Manager" credential, depending on your level of experience, as shown in the table below. You will receive the certificate once you fulfill all the relevant educational and professional requirements.

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

Credential	Exam	Professional experience	Risk management experience	Other requirements
PECB Certified ISO/IEC 27005 Provisional Risk Manager	PECB Certified ISO/IEC 27005 Lead 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 Lead Risk Manager Exam or equivalent	**Two years:** At least one year of work experience in ISRM	At least 200 hours of information security risk management activities	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:** At least two years of work experience in ISRM	At least 300 hours of information security risk management activities	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27005 Senior Lead Risk Manager	PECB Certified ISO/IEC 27005 Lead Risk Manager Exam or equivalent	**Ten years:** At least seven years of work experience in ISRM	At least 1,000 hours of information security risk management activities	Signing the PECB Code of Ethics

General information

- Certification fees and examination fees are included in the price of the training course.
- Participants will be provided with training course materials containing over 450 pages of information, practical examples, quizzes, and exercises.
- An attestation of course completion worth 31 CPD (Continuing Professional Development) credits will be issued to the participants who have attended the training course.
- Candidates who have completed the training course but failed the exam are eligible to retake it once for free within a 12-month period from the initial date of the exam.