



PECB Certified ISO/IEC 27005 Risk Manager

Master the Information Security Risk Management process based on ISO/IEC 27005 and other risk assessment methods

Why should you take this training course?

Information security threats and attacks grow and evolve constantly. As such, organizations are increasingly concerned about how their valuable information is handled and protected. The best form of defense against threats and attacks against to information security is adequate risk management conducted by qualified professionals.

ISO/IEC 27005 Risk Manager training course 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 also gain a thorough understanding of best practices of risk assessment methods such as OCTAVE, EBIOS, MEHARI, and harmonized TRA. This training course corresponds with the implementation process of the ISMS framework presented in the ISO/IEC 27001 standard.

After understanding 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 Risk Manager" credential. By holding a PECB Risk Manager Certificate, you will be able to demonstrate that you have the necessary skills and knowledge to perform an optimal Information Security Risk Assessment and timely manage Information Security risks.



Why is this course more desirable than the others?

This training course teaches how risk assessment for information security is done by combining the information on ISO/IEC 27005 and ISO/IEC 27001. In addition to theoretical knowledge, this training course is equipped with practical exercises, quizzes, case studies, all of which make it a very engaging training course.

This training course with its probing questions and exercises will inspire you to get to know your organization in detail. When focusing on risk management for a successful ISMS, you need to be very clear on what, how, when, why you are doing, and also who will be involved. This training course aims to give you the inquisitive attitude that a good risk manager must have.

What will the certification allow you to do?

Certification is the formal recognition and proof of knowledge which plays an important role when you are entering the labor market, or when you want to advance in your career. Due to the technological advancements and the complexity of cyberattacks, the demand for professionals in information security risk assessment and managing continues to grow. As such, the ISO/IEC 27005 Risk Manager certification has become the norm for best-practice in risk assessment for information security. By obtaining a certification, you showcase a certain skill level which will display added value not only to your professional career but to your organization as well. This can help you stand out from the crowd and increase your earning potential.



Who should attend this training course?

- 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 involved in a risk management program
- IT consultants
- IT professionals
- Information Security officers
- Privacy officers

Course agenda

Duration: 3 days

Day 1 | Introduction to ISO/IEC 27005 and implementation of a risk management program

- Course objectives and structure
- Standard and regulatory framework
- Concepts and definitions of risk
- Risk management program
- Context establishment

Day 2 | Information security risk assessment, risk treatment and acceptance as specified in ISO/IEC 27005

- Risk identification
- Risk analysis
- Risk evaluation
- Risk assessment with a quantitative method
- Risk treatment
- Information security risk acceptance

Day 3 | Risk communication, consultation, monitoring, review, and risk assessment methods

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



Learning objectives

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

Examination

Duration: 2 hours

The “PECB Certified ISO/IEC 27005 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 management framework and process based on ISO/IEC 27005
- Domain 4** | Other information security risk assessment methods

For specific information about exam type, languages available, and other details, please visit the [List of PECB Exams](#) and the [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

General information

- Certification and exam fees are included in the training session price.
- Training material containing over 350 pages of information and practical examples will be distributed.
- An Attestation of Course Completion worth 21 CPD (Continuing Professional Development) credits will be issued to all candidates who have attended the training course.
- In case you do not pass the exam, you can retake it within 12 months following the initial attempt for free.