

Certified ISO 27005 Risk Manager and IEC/ISO 31010 Risk Assessment Methodologies (3 Days)

Mastering risk assessment and optimal risk management in information security based on ISO 27005 and IEC/ISO 31010

Summary

In this three-day intensive course, the participants develop the competence to master the basic risk management elements related to all assets of relevance for information security using the ISO/IEC 27005:2011 and IEC/ISO 31010:2009 standards as a reference framework. Based on practical exercises and case studies, participants acquire the necessary knowledge and skills to perform an optimal information security risk assessment and manage risks in time by being familiar with their life cycle. This training fits perfectly in the framework of an ISO/IEC 27001:2005 standard implementation process.



Who should attend?

- Risk managers
- Persons responsible for information security or conformity within an organization
- Members of the information security team
- IT consultants
- Staff implementing or seeking to comply with ISO 27001 or involved in a risk management program

Learning objectives

- To understand the concepts, approaches, methods and techniques allowing an effective risk management according to ISO 27005 and IEC/ISO 31010.
- To interpret the requirements of ISO 27001 on information security risk management.
- To understand the relationship between the information security risk management, the security controls and the compliance with the requirements of different stakeholders of an organization.
- To acquire the competence to implement, maintain and manage an ongoing information security risk management program according to ISO 27005
- To acquire the competence to effectively advise organizations on the best practices in information security risk management.

Course Agenda

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

- Concepts and definitions related to risk management
- Risk management standards, frameworks and methodologies
- Implementation of an information security risk management program
- Understanding an organization and its context

Day 2: Risk identification and assessment, risk evaluation, treatment, acceptance, communication and surveillance according to ISO 27005

- Risk identification
- Risk analysis and risk evaluation

- Risk assessment with a quantitative method
- Risk treatment
- Risk acceptance and residual risk management
- Information Security Risk Communication and Consultation
- Risk monitoring and review

Day 3: Exam and risk assessment methodologies according to IEC/ISO 31010

- Certified ISO/IEC 27005 Risk Manager Exam (2 hours)
- Brainstorming
- DELPHI technique
- HAZOP – Hazard & Operability Analysis
- SWIFT – The Structured 'What If' Technique
- HACCP - Hazard Analysis Critical Control Point
- Scenario analysis
- FMEA & FMECA analysis
- FTA analysis
- Cause and effect diagram

Prerequisites

None

Educational approach

This training is based on both, theory and practice:

- Sessions of lectures illustrated with examples based on real cases
- Practical exercises based on case studies
- Review exercises to assist the exam preparation
- Practice test similar to the certification exam

To benefit from the practical exercises, the number of training participants is limited

Exam

The "Certified ISO/IEC 27005 Risk Manager" exam fully meets the requirements of the PECB Examination and Certification Program (ECP). The exam covers the following competence domains:

- Domain 1: Fundamental concepts, approaches, methods and techniques of information security risk management
- Domain 2: Implementation of an information security risk management program
- Domain 3: Information security risk assessment based on ISO 27005

The "Certified ISO/IEC 27005 Risk Manager" exam is available in different languages (the complete list of languages can be found in the examination application form)

Duration: 2 hours

For more information about the exam, refer to the PECB section on ISO/IEC 27005 Risk Manager Exam

Certification

After successfully completing the "ISO/IEC 27005 Risk Manager" exam, participants can apply for the credentials of Certified ISO/IEC 27005 Provisional Risk Manager or Certified ISO/IEC 27005 Risk Manager, depending on their level of experience

A certificate will be issued to the participants who successfully pass the exam and comply with all the other requirements related to the selected credential

For more information about the ISO 27005 certifications and PECB certification process, refer to the PECB section on ISO 27005 Risk Manager Certifications

General information

Exam and certification fees are included in the training price

A student manual containing over 400 pages of information and practical examples will be distributed to the participants

A participation certificate of 21 CPD (Continuing Professional Development) credits will be issued to the participants

In case of failure of an exam, participants are allowed to retake the exam for free under certain conditions.

ISO/IEC 27005 and IEC/ISO 31010 are guidance standards on risk management and are not certifiable standards for an organization

More information can be obtained by contacting ISONIKE Ltd at:

Tel. (Office): +357 96 288 534

e-mail: info@isonike.com

Course Approval by:

