ISO 27005: 2011 Risk Manager certification preparation

Seminar of 3 days - 21h
Ref.: AIR - Price 2024: €2 290 (excl. taxes)

EDUCATIONAL OBJECTIVES

At the end of the training, the trainee will be able to:

Understand the concept of risk in relation to information security

Use ISO 27005:2018 for risk analysis

Be aware of other methods (EBIOS RM, MEHARI)

Logically choose a risk analysis method

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@ORSYS.fr to review your request and its feasibility.

THE PROGRAMME

last updated: 07/2021

1) Introduction

- ISO 27000 terminology.
- Definitions of the Threat. Vulnerability. Risks.
- Availability, Integrity, and Confidentiality requirements: Taking into account traceability/evidence.
- Review of regulatory and standards constraints (GDPR, LPM/NIS, PCI DSS, etc.).
- Role of the CISO vs. the Risk Manager.
- The 31000 standard, from interest in an "umbrella" standard to a universal reference source.

2) The concept of "Risk"

- Identifying and classifying risks.
- Operational, physical, and logical risks.
- The consequences of risk (financial, legal, human, etc.).
- Risk management (prevention, protection, risk evasion, transfer).
- Insurability of a risk, financially calculating the transfer to insurance.

3) Risk management according to the ISO

- The method of the 27001:2013 standard and its "Risk Management" process.
- Initially assessment in the Plan phase of section 6: Planning.
- The 27005:2018 standard: Information Security Risk Management.
- Implementing a PDCA process for risk management.
- Context, assessment, treatment, acceptance, and review of risks.
- Steps of risk analysis (identification, analysis, and assessment).
- Preparing the Statement of Applicability (SoA) and the action plan.
- Sharing risks with third parties (cloud, insurance, etc.); Domain 15 of ISO 27002.

4) Risk analysis methods

- MEHARI methods (2010, PRO, and Manager).
- Compliance-based approach vs. risk scenario approach.
- Taking into account sophisticated intentional threats like APTs.
- The goals of EBIOS RM (Identifying the security requirements, Being in compliance, Identifying and analyzing, etc.).
- Activities of the method.

- CRAMM, OCTAVE, etc. History and rest of the world.

5) Conclusion and choosing a method
- How do you choose the best method?
- Knowledge bases (threats, risks, etc.)
- Convergence onto ISO, the need for an update.
- Being or not being in the “ISO spirit”: Constraints of the PDCA model.
- A comprehensive method or project-specific method.
- The real cost of a risk analysis.

DATES

Contact us