Cybersecurity, ISO 27032: Certification

Hands-on course of 5 days - 35h
Ref.: CYB - Price 2024: CHF3 990 (excl. taxes)

EDUCATIONAL OBJECTIVES

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

Know the components and operations of a cybersecurity program in accordance with the ISO 27032 standard

Explain the objective, content, and correlation between ISO 27032 and other standards and frameworks

Master the concepts, methods, standards, and techniques to manage a cybersecurity program

Oversee a cybersecurity program as specified in the ISO 27032 standard

TEACHING METHODS

Lecture course supported by a presentation illustrated with concrete examples, punctuated by discussions, questions, and alternating between theory and practice.

CASE STUDY

Anatomy of an attack on an international telecommunications company. Exercises to identify deviations and handle key concepts.

CERTIFICATION

You will earn PECB “Certified ISO 27032 Lead Cybersecurity Manager” certification if you pass the exam.

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: 06/2022

1) The concepts of cybersecurity and the ISO 27032 standard

- Course objectives and structure.
- Regulatory framework and standards.
- Definition of fundamental cybersecurity concepts.
- Planning a cybersecurity program.

2) Initiating a cybersecurity program

- Organizational structure.
- Defining the roles and responsibilities of cybersecurity agents.
- Establishing the governing policies and principles of cybersecurity.
- Cybersecurity risk management within enterprise risk management.
- Assessing cybersecurity risks.

3) Implementing a cybersecurity program

- Implementing a document management framework.
- Sharing information and coordinating with key players.
- Developing a training program and instructing both staff and key players.
- Implementing specific cybersecurity controls.
- Cybersecurity incident management and integrating it into ordinary incident management.
- Operational Continuity Management.

4) Assessing the performance of the cybersecurity program

- Measuring the return on the actions taken.
- Self-assessment of controls.
- Implementing an assurance environment.
- Assessing the level of cyberthreat preparation.

- Suitability of the implementation of continuous improvement.
- Measuring how fully the cybersecurity controls are integrated into the Information Security controls.
- Overview of the PECB certification system.

5) Taking the certification exam

- Domain 1: Fundamental concepts of cybersecurity.
- Domain 2: Guide to launching, implementing, and managing a cybersecurity program.
- Domain 3: Role and responsibility guidelines for cybersecurity stakeholders.
- Domain 4: Cybersecurity risk management.
- Domain 5: Monitoring activities tied to the cybersecurity program.

Exam : Paper exam with 12 open-ended questions, to be taken in 3 hours, in French. The exam is open-book (you may use course materials and personal notes taken during the session).

DATES

REMOTE CLASS
2024 : 08 Jul, 07 Oct