Publication date : 03/02/2026

Course : Lead Cloud Security Manager, PECB certification

Practical course - 5d - 35h00 - Ref. CSX
Price : 3310 € E.T.

NEW

This training course provides you with the essential knowledge to help set up, manage and improve a cloud security program, based on the ISO/IEC 27017 and ISO/IEC 27018 standards.

Teaching objectives

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

- Understand the concepts, methods and techniques for implementing and managing a cloud security program.
- Understanding the correlation between ISO/IEC 27017, ISO/IEC 27018 and other standards and regulatory frameworks
- Interpret ISO/IEC 27017 and 27018 in the specific context of an organization
- Develop the skills to plan, deploy, manage, monitor and maintain a cloud security program
- Acquire the skills to advise an organization and manage a cloud security program according to best practices

Intended audience

Cybersecurity professionals, managers, consultants and technical experts wishing to set up, manage or improve a cloud security program and master the associated best practices.

Prerequisites

Have a basic understanding of ISO/IEC 27017 and ISO/IEC 27018 and a general knowledge of cloud computing concepts.

Certification

L'examen consiste à répondre à 80 questions, en 3h00 à livre ouvert. À l'issue du cours, une attestation de suivi de la formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation. Les candidats ayant suivi la formation mais échoué à l'examen peuvent le repasser gratuitement une seule fois dans un délai de 12 mois à compter de la date initiale de l'examen.

PARTICIPANTS

Cybersecurity professionals, managers, consultants and technical experts wishing to set up, manage or improve a cloud security program and master the associated best practices.

PREREQUISITES

Have a basic understanding of ISO/IEC 27017 and ISO/IEC 27018 and a general knowledge of cloud computing concepts.

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.

Course schedule

1 Introduction to ISO/IEC 27017 and ISO/IEC 27018 standards and how to set up a cloud security program

- Training objectives and structure.
- Standards and regulatory frameworks.
- Cloud computing concepts and fundamentals.
- Understand the organization's cloud computing architecture.
- Information security roles and responsibilities related to cloud computing.
- Information security policy for cloud computing.

2 Cloud security risk management and cloud-specific measures

- Cloud computing security risk management.
- Selection and design of cloud-specific measures.
- Implementing cloud-specific measures (part 1).

3 Documented information management and cloud security awareness and training

- Implementation of cloud-specific measures (part 2).
- Documented information management in the cloud.
- Cloud security awareness and training.

4 Cloud security incident management, testing, monitoring and continuous improvement

- Cloud security incident management.
- Cloud security testing.
- Monitoring, measurement, analysis and evaluation.
- Continuous improvement.

5 Areas of competence covered by the exam

- Area 1: Fundamental principles and concepts of cloud computing.
- Area 2: Information security policy for cloud computing and documented information management.
- Area 3: Cloud computing security risk management.
- Area 4: Cloud-specific controls based on ISO/IEC 27017 and ISO/IEC 27018.
- Area 5: Cloud security awareness, training, roles and responsibilities.
- Area 6: Cloud security incident management.
- Area 7: Testing, monitoring and continuous improvement of cloud security.

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.

Dates and locations

REMOTE CLASS
2026 : 29 June, 21 Sep., 7 Dec.

PARIS LA DÉFENSE
2026 : 15 June, 14 Sep., 30 Nov.