Publication date : 10/01/2024

Course : ISO/IEC 27035 Lead Incident Manager, PECB certification

Practical course - 5d - 35h00 - Ref. IMC
Price : 3940 CHF E.T.

Cette formation vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation lors de la mise en œuvre d'un plan de gestion des incidents de sécurité de l'information selon la norme ISO/CEI 27035. Durant cette formation, vous découvrirez l'ensemble du cycle de vie de l'incident, de la planification de l'incident aux activités post-incident.

Teaching objectives

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

- ✓ Explain the fundamentals of incident management.
- ✓ Develop and implement incident response plans, select an incident response team.
- ✓ Perform in-depth risk assessments to identify potential threats within an organization.
- ✓ Apply best practices derived from various international standards.
- ✓ Conduct post-incident analysis and identify lessons learned.

Intended audience

Information security incident managers, ICT managers, professional IT systems administrators, professional IT network administrators...

Prerequisites

General knowledge of incident management processes, information security principles and the ISO/IEC 27000 family of standards.

Certification

L'examen consiste à répondre à 12 questions en 3h00 à livre ouvert. À l'issue du cours, une attestation de suivi de la formation de 31 crédits de FPC (Formation professionnelle continue) sera délivrée. 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

Information security incident managers, ICT managers, professional IT systems administrators, professional IT network administrators...

PREREQUISITES

General knowledge of incident management processes, information security principles and the ISO/IEC 27000 family of standards.

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 information security incident management concepts and the ISO/IEC 27035 standard

- Training objectives and structure.
- Standards and regulatory frameworks.
- Fundamental concepts of incident management.
- Information security incident management.
- Setting the context.
- Policies and procedures.

2 Design and preparation of an information security incident management plan

- Risk management.
- Incident management plan.
- Incident management team.
- Internal and external relations.
- Technical and other assistance.
- Information security incident awareness and training.

3 Detecting and reporting information security incidents

- Testing.
- System and network monitoring.
- Detect and warn.
- Gathering information on incidents.
- Information security event reporting.
- Assessment of information security events.

4 Monitoring and continuous improvement of the information security incident management process

- Resolution of information security incidents.
- Containment, eradication and recovery.
- Lessons learned.
- Monitoring, measurement, analysis and evaluation.
- Continuous improvement.

5 Certification

- Areas of expertise covered by the exam :
- Area 1: Fundamental principles and concepts of information security incident management.
- Area 2: Information security incident management process based on ISO/IEC 27035.
- Area 3: Design of an organizational incident management process based on ISO/IEC 27035.
- Area 4: Preparation and execution of the information security incident response plan.
- Area 5: Implementation of off-line information security incident management processes.
- Area 6: Improving incident management processes and activities.

Dates and locations

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.

REMOTE CLASS
2026 : 30 Mar., 15 June, 28 Sep., 7 Dec.