Publication date : 07/09/2024

Course : The fundamentals of IS security

Seminar - 3d - 21h00 - Ref. FTS
Price : 2330 € E.T.

4,2 / 5

BEST

With the explosion of the Internet multiplying development opportunities, information systems security has become a major issue for all companies. This comprehensive training course will introduce you to all the actions and solutions you can take to ensure and improve the security of your information systems. You'll learn what a risk analysis is, how to implement security solutions, and the insurance and legal issues closely linked to the application of a security policy.

Teaching objectives

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

- Understanding the IS risk management process
- Be familiar with reference systems and associated standards
- Learning the legal framework
- Managing the implementation of solutions

Intended audience

Anyone wishing to learn the fundamentals of IS security.

Prerequisites

To have followed the training course "Introduction to computer security".

Course schedule

1 Risk management and safety objectives

- The definition of risk and its characteristics: potentiality, impact, severity.
- The different types of risk: accident, error, malicious intent.
- DIC classification: Availability, Integrity and Confidentiality of information.
- Risk management countermeasures: prevention, protection, risk transfer, outsourcing.

PARTICIPANTS

Anyone wishing to learn the fundamentals of IS security.

PREREQUISITES

To have followed the training course "Introduction to computer security".

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.

2 The CISO's job

- What are the role and responsibilities of the IS Security Manager?
- Towards a safety organization, the role of asset owners.
- How to optimize management of allocated means and resources.
- The Risk Manager in the company, his role in relation to the IS Security Manager.

3 Standards and regulations

- SOX, COSO, COBIT regulations. Who are they for? For whom?
- Towards information system governance. Links with ITIL and CMMI.
- ISO 27001 in an information security management system approach.
- Links with ISO 15408: common criteria, ITSEC, TCSEC.
- The benefits of ISO 27001 certification for organizations.

4 IT risk analysis

- How to identify and classify risks.
- Operational, physical and logical risks.
- How can you build up your own knowledge base of threats and vulnerabilities?
- Methods and standards: EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)/FEROS, MEHARI.
- ISO 27001 risk analysis and the PDCA (Plan, Do, Check, Act) approach.
- What are the contributions of the ISO 27005 standard and developments in French methods?
- From risk assessment to risk management: best practices.

5 The safety audit process

- A continuous, comprehensive process.
- Audit categories, from organizational audits to penetration testing.
- 19011 best practices applied to safety.
- How to create an internal audit program? How do you qualify your auditors?
- Comparative contributions, recursive approach, human implications.
- Safety awareness: who? Who? Who?
- Definitions of Morality/Deontology/Ethics.
- The safety charter, its legal existence, content and validation.

6 The emergency plan and the cost of safety

- Risk coverage and continuity strategy.
- The importance of emergency, continuity, recovery and crisis management plans, PCA/PRA, PSI, RTO/RPO.
- Develop a continuity plan and integrate it into a quality approach.
- How to define safety budgets.
- Definition of Return On Security Investment (ROSI).
- Cost evaluation techniques, different calculation methods, Total Cost of Ownership (TCO).
- The Anglo-Saxon concept of the "Payback Period".

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.

7 Security solutions and architectures

- Selection of suitable safety solutions for each action.
- Definition of a target architecture.
- ISO 15408 as a selection criterion.
- Choosing between IDS and IPS, content control as a necessity.
- How to deploy a PKI project? Pitfalls to avoid.
- Authentication techniques, SSO projects, identity federation.
- The security approach in IS projects, the ideal PDCA cycle.

8 Safety supervision

- How to implement a risk management approach: facts, certainties...
- What are the key indicators and dashboards? Moving towards an ISO and PDCA approach.
- Outsourcing: what's in it for me and what are the limits?

9 Legal aspects

- Reminder, definition of an Automatic Data Processing System (ADPS).
- Types of infringement, the European context, the LCEN law.
- What are the legal risks for the company, its managers and CISOs?

10 Best practices

- Personal data protection, penalties for non-compliance.
- The use of biometrics in France.
- Cybersurveillance of employees: limits and legal constraints.
- Employee rights and employer sanctions.

Dates and locations

REMOTE CLASS
2026 : 8 June, 21 Sep., 23 Nov.

PARIS LA DÉFENSE
2026 : 8 June, 21 Sep., 23 Nov.