Information System Security: Overview

Seminar of 3 days - 21h
Ref.: SSI - Price 2024: CHF2 890 (excl. taxes)

EDUCATIONAL OBJECTIVES

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

Master the security governance process

Use the business frameworks and associated standards of the ISO 27K series

Know the French and European legal framework (LPM, NIS, GDPR, etc.)

Create an action plan to achieve the objectives of the security policy

Develop an appropriate and proportionate response to reduce cyber risks

THE PROGRAMME

last updated: 07/2021

1) Fundamentals of information system security

- The definition of process/information assets and supporting assets (IT).
- The AICT/P classification: Availability, Integrity, Confidentiality and Traceability/Proof.
- The definition of the ISS risk and its specific properties (vulnerabilities, threats).
- Different types of risks: Accident, error, malevolence.
- The emergence of cyber risk, APTs, preparing for a cyber crisis.
- Essential outside sources of information (ANSSI, CLUSIF, ENISA, etc.).

2) The ISS task force: multiple business profiles

- The role and responsibilities of the CISO, the relationship with the IT department.
- Towards a structured and described safety organization, identify competences.
- The role of the asset owners and the need for management to be involved.
- Profiles of architects, integrators, auditors, pen-testers, supervisors, risk managers, etc.
- Building a competent team, trained and responsive to changes in the cyber realm.

3) Standardization and regulatory frameworks

- Incorporating business, legal and contractual requirements. The compliance approach.
- An example of a business regulation: PCI DSS to protect sensitive data.
- Security measures to achieve confidentiality and data integrity.
- An example of legal regulation: NIS directive/France's Military Programming Law.
- The 4 areas of security as seen by the EU and ANSSI: Governance, Protection, Defense, and Resilience.
- Security measures to achieve process availability and integrity.
- The ISO 27001 standard in an information security management system approach (Deming cycle/PDCA).
- The universal best practices of the ISO 27002 standard, the minimum essential knowledge.
- Security areas: from policy to compliance to IT security.
- Developing a Security Assurance Plan in the customer/supplier relationship.

4) The risk analysis process

- Incorporating Risk Analysis into the security governance process.
- Identification and classification of risks, accidental risks and cyber-risks.
- The ISO 31000 and 27005 standards and the relationship of the risk process to the ISO 27001 ISMS.

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.

- From risk assessment to the risk mitigation plan: Best process activities.
- Knowledge of predefined methods: French EBIOS RM approach, U.S. NIST approach, etc.

5) Security audits and the user awareness plan

- Audit categories, from organizational audits to intrusion tests.
- Best practices of the 19011 standard applied to security.
- How to certify your auditors. Example with PASSI in France.
- Security awareness: Who? What? How?
- The need for planned, budgeted awareness.
- Different formats of awareness: Face-to-face or virtual?
- The security charter, its legal standing, its contents, its penalties.
- Quizzes and serious games, for example with the ANSSI MOOC.

6) The cost of security and backup plans

- Security budgets, available statistics.
- The definition of Return On Security Investment (ROSI).
- Cost assessment techniques, different calculation methods, calculating the TCO.
- Hedging risks and the continuity strategy.
- Backup, continuity, recovery, and crisis management plans, BCP/BRP, IT contingency plans, RTO/RPO.
- Developing a continuity plan, fitting it into a security approach.

7) Designing optimal technical solutions

- Structuring its logical and physical protection. How to develop defense in depth.
- The three main areas of computer security (networks, data, software).
- Partitioning your sensitive networks, network and application firewall technologies.
- Make your data unreadable during storage and transport, cryptographic techniques.
- Securing your software through hardening and secure design.
- Software vulnerability management, how to use CVE/CVSS.

8) Security monitoring

- Operational indicators for governance and security.
- Cyber management: ISO-compliant dashboard.
- Preparing your defense (IDS, incident detection, etc.).
- Alert processing and cyber forensics, the role of CERTs.

9) Violations of law relating to Automatic Data Processing Systems

- Legal definition in France of an Automatic Data Processing System (STAD).
- Types of violations, European context, the LCEN law. The GDPR regulation.
- What legal risks are there for the company, its leaders, the CISO?

10) Recommendations for “legal” IS security.

- Personal data protection, penalties for non-compliance.
- Use of biometrics in France.
- Employee cybersurveillance: Legal limits and restrictions.
- Employee rights and penalties incurred by the employer.

DATES

Contact us