Publication date : 02/24/2026

Course : CISO (Information System Security Manager), level 1

Synthesis course - 4d - 28h00 - Ref. RSD
Price : 3130 CHF E.T.

NEW

CISO training prepares professionals to manage the security of information systems, by covering technical skills (regulatory framework, technical solutions, etc.).

Teaching objectives

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

- Mastering the security governance process
- Using the ISO 27K series of business repositories and associated standards as a CISO
- Know the French and European legal framework (LPM, NIS, RGPD...)
- Plan actions to achieve safety policy objectives
- Develop an adequate, proportionate response and reduce cyber risks, including associated technical measures
- Understanding IS security supervision processes

Intended audience

Engineers taking on the role of CISO, IT directors or managers, security engineers or correspondents, project managers integrating security constraints.

Prerequisites

No special knowledge required.

Course schedule

PARTICIPANTS

Engineers taking on the role of CISO, IT directors or managers, security engineers or correspondents, project managers integrating security constraints.

PREREQUISITES

No special knowledge required.

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.

1 The fundamentals of information system security

- Security principles: defense in depth, cyber risk modeling.
- DICT/P classification: Availability, Integrity, Confidentiality and Traceability/Proof.
- The emergence of cyber-risk, the evolution of cybercrime.
- The course of a cyber attack (Kill Chain).
- Key external sources of information (ANSSI, CLUSIF, ENISA, etc.).
- Security objectives: confidentiality, availability, data integrity and traceability.

2 The SSI task force: multiple business profiles

- The role and responsibilities of the CISO, and the relationship with the IT Department.
- Towards a structured and described safety organization, identifying skills.
- The role of asset owners and the need for management involvement.
- Profiles for architects, integrators, auditors, pen-testers, supervisors, risk managers, etc.
- Build a team that is skilled, trained and responsive to changes in cyberspace.

3 Normative and regulatory frameworks

- Integrating business, legal and contractual requirements. The compliance approach.
- Security domains: from policy to compliance and IT security.
- An example of legal regulation: NIS directive/ Military Planning Law.
- RGPD and the role of the CISO.
- The 4 axes of security as seen by Europe and ANSSI: Governance, Protection, Defense and Resilience.
- ISO 27001 in a management system approach (Deming/PDCA wheel).
- ISO 27002 universal best practices, the minimum knowledge required.
- Draw up a safety assurance plan for customer/supplier relations.
- Cyber management: ISO compliant dashboard.

4 The risk analysis process

- Integrating risk analysis into the safety governance process.
- Identifying and classifying risks, accidental risks and cyber risks.
- ISO 27005 standards and the relationship of the risk process to the ISO 27001 ISMS.
- From risk assessment to risk treatment plan: the right process activities.
- Familiarity with predefined methods: FR/EBIOS RM approach, US/NIST approach, etc.

5 Raising user awareness

- Safety awareness: Who? Who? What? How?
- The need for programmed, budgeted awareness-raising.
- The different awareness-raising formats: face-to-face or virtual?
- The safety charter, its legal existence, content and sanctions.
- Quizzes and serious games, such as the ANSSI MOOC.

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.

6 Designing optimal technical solutions - Data security

- Cryptographic techniques.
- Public key and symmetrical algorithms.
- Simple, salt and key (HMAC) hash functions.
- Public key architectures (PKI).
- Application of cryptography: TLS exchanges, security of data at rest ...
- Backup strategy (BCP, DRP, etc.).

7 User authentication and authorization

- IAM, a major challenge.
- Biometric authentication and legal aspects.
- Authentication techniques (passwords, certificates, UAF and U2F standards from the FIDO (Fast ID Online) alliance).
- Various attack techniques (brute force, keylogger, credential stuffing, etc.).
- Strong multi-factor authentication (MFA).
- OATH's HOTP and TOTP standards.

8 Designing optimal technical solutions - Network security

- Partitioning sensitive networks, network and application firewall technologies.
- LAN security: Vlans, NAC ...
- Differences between UTM, enterprise, NG and NG-v2 firewalls.
- The risks associated with Cloud Computing according to CESIN, ENISA and CSA.
- The Cloud Controls Matrix and its use in evaluating Cloud providers.
- CASB solutions for securing data and applications in the cloud.
- Administration network security: SSH, bastioning, partitioning and best practices.
- Wireless network risks and best practices.
- VPN solutions.

9 Designing optimal technical solutions - Workstation and server security

- Understand endpoint threats.
- Anti-virus/anti-spyware software.
- Malware: payloads (ransomware, exploits), propagation (drive-by downloads, malicious USB keys).
- Hardening principle.
- How to secure removable devices?
- Virtual architecture vulnerabilities and best practices.
- Smartphone safety and best practices.

10 Active safety management and supervision

- Audit categories, from organizational audits to penetration testing.
- Intrusion tests (black box, gray box and white box).
- How do you qualify your auditors? - example with PASSI in France.
- Supervision strategy: log, IPS (Intrusion Prevention System) and IPS NG.
- Implement a SIEM solution.
- Implement or outsource your Security Operation Center (SOC).
- Incident response procedures and crisis management.

Dates and locations

REMOTE CLASS
2026 : 26 May, 8 Sep., 24 Nov.