Publication date : 02/17/2025

Course : Implementing, governing and certifying an NIS 2 project

Achieving NIS v2 compliance successfully

Seminar - 2d - 14h00 - Ref. NIS

Price : 2170 CHF E.T.

4,6 / 5

The aim of the NIS 1 (Network and Information System 1) directive was to develop cybersecurity throughout the European Union, to mitigate threats to networks and information systems used to provide essential services in key sectors, and to guarantee the continuity of these services in the event of incidents. In so doing, it contributes to the security of the Union and the smooth functioning of its economy and society. The NIS 2 directive is part of a reinforced and necessary continuity in the face of an expanding cyberthreat landscape and the emergence of new challenges.

Teaching objectives

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

- Understanding cyber risk issues and European responses
- Integrate the security reference framework defined by the French government for the NIS directive
- Understanding the changes between NIS 1 and NIS 2
- Learn how to implement and deploy them through case studies
- Understanding the ANSSI certification process
- Evaluate project implementation costs

Intended audience

CISOs and security advisors, security architects, IT directors and managers, IT engineers, project managers (MOE, MOA), security auditors and IT regulatory lawyers.

Prerequisites

Basic knowledge of cybersecurity or knowledge equivalent to that acquired in the BYR and SSI seminars.

Course schedule

PARTICIPANTS

CISOs and security advisors, security architects, IT directors and managers, IT engineers, project managers (MOE, MOA), security auditors and IT regulatory lawyers.

PREREQUISITES

Basic knowledge of cybersecurity or knowledge equivalent to that acquired in the BYR and SSI seminars.

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 Introduction: the challenges of European cybersecurity

- Sensitive data: cyber theft, espionage, sabotage...
- New Cold War East/West, USA/China, West/Russia.
- Organized hackers, the role of intelligence agencies.
- APT (Advanced Persistent Threat), ransomware, targeted risks.
- The approach to cyberthreats: towards a "cyber Schengen"?

2 The essentials for CISOs

- For whom: essential and important entities, new eligibility and exclusion criteria.
- For which ecosystems? New business sectors and ESNs.
- Which rules? Of the 23 rules of NIS 1 plus "what it lacked".
- When? From 2024 to 2026...
- How can we help? With a controlled governance and certification process.
- What penalties? Graduated on sales, based on the example of the RGPD.

3 Safety measures

- NIS governance, protection, defense and resilience rules 1.
- Risk analysis and information systems security policies.
- Incident management.
- Business continuity and recovery, crisis management.
- Supply chain security.
- Security in the acquisition, development and maintenance of networks and information systems.
- Assessing the effectiveness of cybersecurity risk management measures.
- Basic cyber hygiene practices and cyber security training.
- Policies and procedures for the use of cryptography and, where applicable, encryption.
- Human resources security, access control policies and asset management.
- The use of multi-factor or continuous authentication solutions.

4 Compliance project management

- From gap analysis to compliance.
- Governance by risk: relevance of EBIOS RM in an NIS project.
- Repetition of existing security measures, and NIS 1 rules where applicable.
- The ANSSI certification process adapted to the NIS 2 directive.
- NIS 2 project milestones and resources.

5 Conclusion: on the road to certification

- Strong ISO 27K inspiration: link with ISO 27001 and new ISO 27002:2022 best practices.
- Consistent cyber-resilience: link with DORA and CER directives and regulations.
- French transposition: the parallel evolution of the LPM and OIV.
- Differentiated state controls (ex ante or ex post regulation).
- A penalty process comparable to the RGPD, the rules for the graduation of fines.
- The security of its ecosystem and critical stakeholders.

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 : 26 Mar., 16 June, 1 Oct., 8 Dec.