Publication date : 04/18/2024

Course : Cybersecurity frameworks and standards: understand, compare and choose effectively

NIS 2, NIST CSF 2, ISO 27001:2022, PCI DSS, SecNumCloud...

Seminar - 2d - 14h00 - Ref. NST

Price : 2170 CHF E.T.

4,5 / 5

The fight against cybercrime, an essential component of IS control, has seen an explosion in the publication of best practice and requirements guidelines. Faced with this multiplicity of tools, the aim of this seminar is to provide a broad overview of the available standards, and to clarify their scope and specificity, in order to guide the choice of those in charge of cybersecurity. You'll see what questions you need to ask yourself as you make your choices and face up to the growing cyber threat.

Teaching objectives

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

- Understanding cyber risk issues and responses State of the art
- Learn about the main international cybersecurity standards
- Integrating security guidelines into IT best practices
- Learn about the implementation and deployment of repositories through case studies
- Compare and choose the most effective way to achieve your safety objectives
- Understand the certification/compliance and homologation processes
- Evaluate implementation costs as part of a global information system

Intended audience

CISOs or security correspondents, security architects, IT directors or managers, engineers, project managers (MOE, MOA), auditors who have to integrate security requirements.

PARTICIPANTS

CISOs or security correspondents, security architects, IT directors or managers, engineers, project managers (MOE, MOA), auditors who have to integrate security requirements.

PREREQUISITES

Basic knowledge of cybersecurity, or knowledge equivalent to that provided by BYR or SSI courses.

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.

Prerequisites

Basic knowledge of cybersecurity, or knowledge equivalent to that provided by BYR or SSI courses.

Course schedule

1 The European model: Network Information Security 2 (NIS 2)

- New Cold War East/West, USA/China West/Russia.
- Organized hackers, the role of intelligence agencies.
- APT (Advanced Persistent Threat), ransomware, targeted risks.
- Mapping reference systems: from specialist to generalist.
- European cybersecurity issues.
- Areas of application EE, EI, OSE, FSN, new eligibility criteria.
- For which ecosystems - New business sectors and ESN/IT enlisted.
- The most important security measures: from the 23 rules of NIS 1 and many more...
- The risk governance and controlled certification process.
- The system of graduated sanctions on CA, like the RGPD.

Case study

Deploy an NIS 2 project, starting from NIS v1, with the aim of certification.

2 The American model: NIST CSF 2.0

- The core with its set of categories and sub-categories.
- The new GOVERN function and its relevance to strategic cyber governance.
- 800 and 1800 series implementation guides in support of the CSF.
- Framework implementation levels: tiers 1 to 4.
- Learn how to scale your security according to your objectives and the criticality of your activities.
- Integrate secure development with the complementary SSDF framework.
- Create your own profile based on business safety objectives and stakeholder requirements.
- Build a profile of cyber threats to the ecosystem.

Case study

Deploying a governance profile with the new NIST CSF 2.0

3 The universal ISO 27001:2022 model

- ISO 27001 in a management system approach (Deming/PDCA wheel).
- ISO risk governance: ISO 31000/ISO 27005.
- Drawing up a risk management plan and declaration of applicability.
- The universal best practices of ISO 27002:2022.
- Safety domains and attributes associated with the 93 measures.
- Build a document management and evidence base.
- Understand the ISMS audit process (first-party and third-party).

Case study

Deploy a continuous improvement dynamic with ISO 27001.

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.

4 SecNumCloud IT cloud model

- ANSSI's vision of secure cloud computing and its latest developments for 2023.
- Key best practices for protecting and defending trusted hosting sites.
- A security label encompassing ISO 27001 and ISO 27017/27018 for a sovereign cloud.
- Protection against non-European laws.
- Towards a European qualification for EUCS cloud computing service providers?

5 A model for healthcare: HDS (healthcare data hosts)

- The HDS standard: ISO 27001 as a foundation.
- Health data: protection requirements and the link with the RGPD.
- Additional requirements.
- Certification framework for hosting companies.

6 A model for finance/payment : PCI DSS v4

- The PCI card payment industry and its requirements frameworks.
- The main players in the sector: brands, banks, merchants, PSPs.
- The ecosystem of PCI players : QSA, ASV, certified publishers...
- Specific cyberthreats to CB data: theft, skimming.
- Managing a project through to compliance, first steps with the SAQ.

7 Safety according to COBIT®, ITIL® and ITIL®.

- COBIT®: a framework for aligning IT governance with business objectives.
- COBIT® risk management processes.
- Organizational and HR models.
- COBIT® security principles.
- Safety control templates.
- ITIL®: a framework for IT service delivery.
- ITIL® processes.
- The Information Security Management process.
- ITIL® and its links with ISO 27001.

8 Which strategy to choose?

- Advantages and disadvantages of each reference system.
- Comparison and selection criteria.
- Hybrid and complementary approaches.
- Comparative costs and multi-referential alignments.

Dates and locations

REMOTE CLASS
2026 : 10 June, 1 Oct., 8 Dec.