+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 05/17/2025

Sign up

# Training NIS 2 Directive: new European cybersecurity standards

2 days (14 hours)

## Presentation

Our Network and Information Security 2 (or NIS 2) directive training course will bring up to speed on the latest European security directives. This directive follows on from NIS 1, created in 2016 to strengthen cybersecurity within the European Union. It will be mandatory from 2024, and reinforces the measures taken by member states that companies will have to comply with.

Our NIS 2 training course will give you a head start on the implementation of this directive in the European area, and ensure that your company is ready for the forthcoming European standards.

In this training course, you'll learn about all the changes compared to the previous NIS Directive. You'll learn about all the new measures introduced by the European Union in terms of cybersecurity, with a broader scope of application and much greater collaboration between the various European states.

## Objectives

- Understand what's new in NIS 2.
- Adapt company processes to new regulations.

## Target audience

- CEO
- Cybersecurity managers

## Prerequisites

Knowledge of NIS 1 is a plus, but not essential

# NIS 2 Directive training program

## Introduction to European CyberSecurity

- Current issues: cybervols, espionage, sabotage
- Geopolitical dynamics: East/West tensions, USA/China, West/Russia
- Cyberthreat actors: hackers, intelligence agencies, APTs and ransomware
- Towards enhanced European cooperation: the idea of a cyber-Schengen

## Role and responsibilities of the CISO under NIS 2

- Targeting entities: criteria for essential and important entities
- Affected areas and ecosystems
- Regulations: developments since NIS 1 and new requirements
- Application timetable: from 2024 to 2026
- Implementation: governance processes and certification
- Potential penalties: model inspired by the RGPD

## Implementing Security Measures

- NIS 1 policy review: governance, protection, defense, resilience
- Risk analysis and information systems security
- Incident management and business continuity
- Security in the supply chain and in systems development
- Cybersecurity assessment and continuous improvement
- Practical measures: cyber hygiene, use of cryptography and multi-factor authentication

## Compliance Project Management

- From preliminary analysis to compliance: integrating EBIOS RM assessments
- Adapting pre-existing safety measures and risk governance
- NIS 2-specific certification process and ANSSI's role
- Planning and resources for the NIS 2 compliance project

## Conclusion: Towards certification and beyond

- Integration of ISO 27001 standards and ISO 27002:2022 best practices
- Cyber resilience and alignment with DORA and CER directives
- National transposition: changes to the LPM and regulation of OIVs
- State control and sanction management: approaches and gradation of sanctions
- Securing the ecosystem and interactions with stakeholders

## Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

## Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

## Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

## Organization

The course alternates theoretical input from the trainer, supported by examples, brainstorming sessions and group work.

## Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

## Sanction

A certificate will be issued to each trainee who completes the course.