AMBIENT IT

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

Updated on 29/11/2023

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 you 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 enable you to get a head start on the implementation of this directive in the European area, and thus ensure that your company is ready for the forthcoming European standards. In this training course, you'll learn about all the changes compared with 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

- Fields of application
- Essential entities
- Cybersecurity in the EU
- Member States' strategies
- New risk management measures
- New obligations

National security strategy

- Tour of the competent authorities
- State frameworks for cybercrisis management
- Response teams and CSIRT
- European vulnerability database
- EU-CyCLONE and large-scale crises

Risk management measures

- Governance
- Management bodies of key entities
- Cybersecurity risk management measures
- Declaration obligation

Jurisdiction and territoriality

- Entities and Jurisdiction
- Non-European entities
- Representative duties
- Major and essential entities
- Sanctions

Extraterritoriality

- Extraterritorial application of Community law
- Risk management
- Master plan
- european directives and conformity issues
- **Cyber resilience**, DORA and CER

DORA

- Governance and organization
- Internal control frameworks
- ICT risk
- ICT audits
- Resilience test

CER

- Fields of application
- Resilience strategy for critical entities
- Significant disruptive effects
- Incident notification
- Member State cooperation

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, with 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.