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

Updated on 16/01/2025

Sign up

Training: DORA Digital Operational Resilience Act

2 days (14 hours)

Presentation

Our Digital Operational Resilience Act (DORA) training course will help you master the ins and outs of this new European regulation, and ensure that your organization complies with it. Financial institutions must now follow a whole set of rules around incidents linked to new technologies.

Our program will give you a detailed understanding of the European Union's legislative context and the institutions involved in its application. You will learn how to establish an ICT risk management framework, detection methods, incident response and disaster recovery.

Our training will also enable you to conduct resilience tests within your organization. You'll learn about the crucial role of testers in threat-driven penetration testing (TLPT).

Finally, the role of the competent authorities and cross-sector cooperation will be discussed, as will data protection and professional secrecy in the DORA.

Objectives

- Understanding DORA principles
- Apply regulations to your organization
- Conducting resilience tests

Target audience

- **CEO**
- Project managers
- Managers
- DPO

Prerequisites

- Knowledge of the financial institutions sector

Digital Operational Resilience Act TRAINING PROGRAM

INTRODUCTION AND EU LEGISLATIVE CONTEXT

- Presentation of the Digital Operational Resilience Act (DORA) and its importance
- Understanding the European Union's legislative process
- Key institutions involved in the creation of DORA
- Relationship between DORA and other regulations such as the NIS 2 directive
- Overview of European legislation and its impact on DORA

TIC RISK MANAGEMENT

- Establishing an ICT risk management framework
- Identification, protection and prevention
- Detection, response and recovery methods
- Importance of backup policies and restoration procedures
- Communication and harmonization of ICT risk management tools

ICT INCIDENT MANAGEMENT

- ICT incident management process and incident classification
- Major incident reporting and notification of significant cyber threats
- Harmonization of reporting content and templates
- Implications of supervisory feedback in the event of incidents

DIGITAL OPERATIONAL RESILIENCE TESTING

- General requirements for resilience test performance
- Advanced testing of ICT tools and systems
- Importance and role of testers in threat-driven penetration testing (TLPT)

THIRD-PARTY RISK MANAGEMENT TIC

- Risk management principles for ICT third parties
- ICT concentration risk assessment and essential contractual provisions
- Monitoring framework for critical third-party ICT service providers
- Roles and powers of senior supervisors in the context of surveillance

COOPERATION, SANCTIONS AND FINAL PROVISIONS

- Roles of competent authorities and cross-sector cooperation
- Cross-sector financial exercises and communication
- Remedial measures and administrative sanctions
- DORA revision clauses and transitional provisions
- DORA data protection and professional secrecy

FAQ - QUESTIONS / ANSWERS

Why are DORA regulations necessary?

With the multiplication of technologies in the financial sector, vulnerabilities have also become more numerous. Poor risk management can have catastrophic consequences for the global economy. It was to ensure the resilience of the financial sector on a European scale that the DORA regulation was created.

How does DORA training work?

Our training obviously covers the theoretical aspects needed to learn the regulations, but it also includes MCQs and role-playing exercises to ensure that all the concepts covered are properly understood.

What will DORA Training do for me?

On completion of this course, you will be able to implement and manage ICT risk management framework in full compliance with DORA requirements.

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 on entry to training complies with Qualiopi quality criteria. As soon as enrolment is confirmed, the learner receives a self-assessment questionnaire enabling us to

assess their estimated level of proficiency in different types of technology, and their 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) that 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.