Publication date : 10/14/2024

Course : DORA (Digital Operational Resilience Act), implementing a digital resilience strategy

Seminar - 2d - 14h00 - Ref. DRA
Price : 2120 CHF E.T.

4,3 / 5

The DORA standard is a European regulatory framework designed to strengthen the operational resilience of financial entities in the face of IT and cybersecurity risks. It imposes strict requirements in terms of IT risk management, cybersecurity testing, incident management and critical infrastructure resilience. By harmonizing standards across the EU, DORA ensures greater protection against cyber threats, limiting disruptions to financial services and strengthening digital confidence.

Teaching objectives

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

- Understand the main objectives and key concepts of the DORA regulation
- Understanding the different types of cyber risks
- Identify data security and regulatory compliance obligations
- Learn about digital security best practices and raise employee awareness
- Setting up and implementing a digital resilience strategy

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 and information systems security.

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 and information systems security.

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 Information and communication technology (ICT) risk management

- DORA provisions reminding us of the need to implement an ICT risk management system.
- Key principles and requirements for financial entity risk management.
- Obligations relating to the ICT risk management framework.

2 Management, classification and reporting of ICT incidents

- Provisions of the DORA regulation aimed at harmonizing and streamlining the reporting of ICT incidents.
- Classification and reporting of ICT incidents.
- Notification of major ICT incidents to the competent ESA (European Supervisory Authorities).
- Voluntary notification of major cyber threats to authorities such as EBA, EIOPA and ESMA.

3 Digital operational resilience testing

- Digital operational resilience tests on the most critical parts of their information systems.
- Advanced testing based on Threat-Led Penetration Testing (TLPT).
- Large-scale live threat testing by independent testing organizations.

4 Managing risks related to third-party service providers

- Third-party risk management principles for ICT risk management.
- Provisions to be taken into account when dealing with third-party service providers supplying ICT services.
- Europe-wide monitoring framework for critical third-party ICT service providers.

5 Information exchange provisions

- Strengthen the digital operational resilience of financial entities.
- Voluntary exchange of information and intelligence on cyber threats between different financial entities.

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 : 17 Mar., 28 May, 13 Oct., 26 Nov.