# Training sheet
# The DORA regulation on digital operational resilience

## CONTACT FOR THIS TRAINING SESSION

Miora RAHARINIRINA
Training Manager
almond.institute@almond.eu
07 64 42 71 56

- Version 1.0
- 29/07/2024

# The DORA regulation on digital operational resilience

## Course overview

This training course is designed to meet the requirements mentioned in article 5.4 of the DORA regulation. It aims to provide management bodies with the knowledge and skills they need about governance, contracts with ICT service providers, ICT risk management and the impact on operations.
It includes:

- Cyber news as it is induced by DORA
- The fundamentals of DORA
- A reminder of the "Risks - Measures - Controls" trio and the essentials of Cyber risk management
- What it takes to move your organization towards compliance

01. **Understand** the main objectives of the DORA regulation

02. **Make** management **accountable** for meeting regulatory obligations

03. **Identify** matrix concepts and notions

04. **Master** the impact of the DORA regulation on contracts (pre-contractual phase and dedicated clauses)

# The DORA regulation on digital operational resilience

## Useful informations

### Who should attend?

- Top management
- Any collaborator involved in the DORA regulation, on an occasional or permanent basis

### Entry requirements

- No prerequisites

### Method of assessment

End-of-session quiz to assess the knowledge acquired

### How and when to access

The trainee is considered registered when :

- Prerequisites and requirements have been identified and validated
- Training agreement signed

**Registration requests can be sent up to 10 working days before the start of the course**.

### Accessibility

Whether you are recognized as disabled or not, making our training accessible to everyone is part of our commitment.

If you need compensation or adaptation regarding the content, media, “place”, equipment used, timetables or tempo, **we're here to help**.

# The DORA regulation on digital operational resilience

## Face-to-face and distance learning

## Course curriculum

| ICT risk management | ICT incident reports | Digital operational resilience test | Risk management for third-party ICT service providers | Sharing information and intelligence |
|---|---|---|---|---|
| → Limit disruption caused by incidents with appropriate risk management and monitoring systems<br>1. Document the ICT risk management framework<br>2. Identify the most critical service providers<br>3. Mapping risks to establish mitigation measures | → Enhance the ICT incident management system to ensure an effective response to current threats<br>1. Update and improve existing systems using monitoring and testing data | → Test the effectiveness of the ICT risk management framework by testing systems and responding to threats with minimum impact<br>1. Document the methods implemented to counter risks and achieve resilience objectives<br>2. Document business continuity and recovery plans<br>3. Conduct penetration tests | → Propose a holistic vision of the management of ICT service providers, particularly providers of critical and important functions<br>1. Document a risk strategy for third-party ICT service providers<br>2. Comply with the pre-contractual requirements : identification and assessment<br>3. Set minimum contractual requirements<br>4. Update a register of contracts related to ICT service providers | → Define a communication strategy to promote the sharing of information on cyber threats between financial entities<br>1. Gather informations on cyber threats<br>2. Contribute to information sharing between financial entities<br>3. Train managers and employees on digital operational resilience |

## Training benefits

- → Industry-specific training provided by a regulatory compliance expert and by a lawyer with expertise in IT, compliance and security
- → Recommandations and keys for what's next

## Prices and informations

- → **Duration:** 2h
- → **Price:** Contact us
- → **Funding:** Support from OPCO

→ READ MORE