Getting Ahead of DORA: Essential Actions for Trustees

28 November 2024

Agenda

1. Introduction to DORA
2. Trustee Responsibilities Under DORA
3. Key DORA Compliance and Timing
4. Key Takeaways and Next Steps for Trustees
5. Q&A

Naomi Reville
DORA Trustee Engagement Lead & Senior Consultant
+353 (0)1 963 8267
naomi.reville@lcp.com

Introduction to DORA

Enhancing the Operational Resilience of the EU Financial Sector

What is DORA?

- EU regulation aimed at strengthening the operational resilience of the financial sector, particularly against ICT (Information and Communication Technology) risks

Purpose?

- Ensure that financial institutions, including pension schemes, can withstand, respond to, and recover from ICT-related disruptions

Why?

- Information Communication Technology (ICT) is used to support every-day activities
- Increasing cyber threats: Protect essential functions
- ICT incidents have the potential to jeopardise the stability of the entire financial system

Who?

- DORA applies to financial institutions in the EU, including pension schemes with more than 15 members
- Accountability for compliance with DORA is established at management level - for pension schemes, with the scheme trustees

How?

Five-Pillar Framework:

1. ICT Risk Management
2. ICT-related Incident Reporting
3. Digital Operational Resilience Testing
4. Third-Party Risk Management
5. Information Sharing

Trustee Responsibilities Under DORA

Trustee Responsibilities:

1. Comprehensive ICT risk management
2. Identify sources of ICT risk, and monitor security and functioning of ICT systems
3. Third-party risk management
4. Maintain a Register of Information of ICT third-party service providers
5. Incident management and reporting
6. Regular resilience testing

Defining ICT Third-Party Service Providers

Awaiting Clarification

ESAs DORA 2024 Dry Run FAQ – update published July 2024:

"In case a financial entity is the service provider, the single exception to recital 7 is about services for which the financial entity must be authorised/licenced/registered as financial entity to deliver it: in that case such services are therefore regulated financial services and not an ICT service in the meaning of DORA Article 3(21). Financial entities would need to make their own assessment".

On 29th July, the ESAs issued the following:

"Consistently with DORA Article 3(19), all third-party service provider providing ICT services to a financial entity are considered as ICT third-party service provider.

Given the number of questions received on the interpretation of ICT services and ICT service providers received from stakeholders requiring a legal interpretation, in order to provide legal certainty, the ESAs having liaised with the European Commission have agreed to respond to these questions via a formal Q&As in due course. For the time being, the financial entities are invited to register their contracts on a best effort basis taking into account that the Register of Information is also an ICT third-party risk management tool."

Key DORA Compliance and Timing

DORA Regulation: Comes into effect on 17 January 2025

1. Policies and Frameworks – 17 January 2025

- All required ICT risk management frameworks, policies, and governance structures.
- Key documents include:
  - Digital Operational Resilience Strategy
  - ICT Governance and Control Framework
  - ICT Risk Management Framework

Item	Frameworks and Policies
1	ICT Governance and Control Framework
2	Digital Operational Resilience Strategy
3	Digital Operational Resilience Testing Policy
4	ICT Risk Management Framework
5	Use of ICT Services Policy
6	ICT Third-Party Provider Contract & Exit Strategy Policy
7	ICT Asset Management Policy
8	ICT Response and Recovery Plan
9	Incident Management Process
10	ICT Business Continuity Policy
11	Reporting and Communication Policy
12	ICT Training and Learning Policy

Key DORA Compliance and Timing

DORA Regulation: Comes into effect on 17 January 2025

2. Third Party Providers – 17 January 2025

- Develop a map of third-party service providers and the critical or important functions they support.
- Engage with third-party providers about their DORA compliance readiness and document outcomes
- Review and update third-party contracts to include DORA required clauses

Business Function	XX Pension Plan
Administration	
Actuarial	
Risk Management KFH	
Internal Audit KFH	
Investment Management	
Custodian	
Consultancy	
Scheme Secretarial	
Legal advice	
External auditor	
Life Insurance	
Trustee Bank Account	

Critical or Important Function

Article 3 (22) of the Digital Operational Resilience Act (DORA) (Regulation (EU) 2022/2554) states:

"'critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law"

Key assessment criteria:

- Impact on operational continuity
- Impact on financial stability
- Market integrity and consumer protection
- Compliance with legal and regulatory requirements
- Interdependencies
- Substitutability
- Impact on outsourced functions

Key DORA Compliance and Timing

DORA Regulation: Comes into effect on 17 January 2025

3. Registers of Information: TBC

Original Submission Date: 17 January 2025

ESAs Extended Submission Date: 30 April 2025
First submission to the European Supervisory Authorities (ESAs) must occur by this date.

Pensions Authority Submission Date: TBC
The Pensions Authority deadline for collecting Registers is to be announced.

Key Takeaways and Next Steps for Trustees

Key Takeaways

- Trustees are accountable for implementing robust ICT risk management frameworks, policies, and processes.
- Initial DORA compliance deadlines are approaching (January 17, 2025), with extensions for Registers of Information.

Next Steps for Trustees

- Finalise and approve ICT risk management policies and frameworks.
- Develop a map of third-party service providers and the critical or important functions they support
- Engage third-party providers to assess their DORA readiness and update contracts.
- Prepare and maintain Registers of Information for ICT third-party service providers.
- Stay informed about upcoming guidance and Q&As from the ESAs.

Questions & Answers