NORTH HOUSE

DORA AND THE REGISTER OF INFORMATION

An overview of Dora and the Dora Register of Information.

02

ABOUT DORA

Strengthening Digital Foundations in Finance: The Digital Operational Resilience Act (DORA) introduces a crucial step forward in safeguarding the financial sector against digital disruptions. Central to DORA's strategy is a detailed record keeping requirement, known as the Register of Information (RoI), which encourages financial institutions to systematically record their external technology providers

DORA IN SHORT

03

What is it about?

Strengthen Resilience: To ensure that the financial sector can withstand, respond to, and recover from all types of ICT disruptions and threats.

Regulatory Clarity: To provide a comprehensive regulatory framework that addresses digital operational resilience for financial entities, consolidating various existing regulations into a unified approach.

Harmonization: To harmonize digital operational resilience testing across the EU for critical entities in the financial sector.

Risk Management: To enforce effective ICT risk management capabilities, encompassing preventative measures, mitigation strategies, and recovery plans from ICT incidents.

Third party risk management: To provide rigorous oversight and management of risks associated with third-party ICT service providers across supply chains, docmented as the RoI.

Who is affected by Dora?

DORA applies to a wide array of financial entities within the EU, including but not limited to:

- Banks
- Insurance Companies
- Investment Firms
- Crypto-asset Service Providers
- Critical Third-Party Providers, such as cloud computing services

These entities are required to maintain robust digital operational frameworks to manage ICT risks effectively.

04

IMPACT AND PENALTIES

Failing to comply with DORA regulations can lead to severe consequences, such as substantial fines. These penalties are designed to ensure strict compliance with operational resilience practices, highlighting the essential role of ICT security within the financial sector.

To avoid the risks associated with non-compliance, it is essential for affected entities to assess their current ICT resilience strategies and begin preparations to fully meet the forthcoming regulatory demands.

05

DORA REGISTER OF INFORMATION

The Purpose of Dora Register of Information

Under DORA, a key requirement for financial entities is to maintain a comprehensive "Register of Information." This register serves several critical functions:

- **Monitoring ICT Third-Party Risk:** Helping financial entities systematically monitor risks associated with their technology providers.
- **Supervisory Review:** Assisting EU competent authorities in supervising ICT and third-party risk management practices at financial entities.
- **Critical Provider Designation:** Enabling the European Supervisory Authorities (ESAs) to designate critical ICT third-party service providers subject to EU-level oversight.

For official guidelines, visit the European Supervisory Authorities' website .

This structured register must be fully prepared and ready to submit in **early 2025.**

To ensure that financial entities are prepared with their information registers by January 2025, the ESAs and competent authorities will conduct a preliminary test beginning in May 2024, on a best-efforts basis.

07

Technical Specifications, Formal Requirements and Reporting format

The Register of Information includes - among other- the following:

- **Service Details:** Provider identities, services provided, and their importance to the institution.
- **Contractual Agreements:** Details such as costs, start, and end dates of contracts.
- **Risk Assessments:** Evaluations of potential risks associated with each ICT service.
- **Operational Links**: Documentation of how these services integrate with the financial entity's operations.

However, the Register of Information (RoI) involves several complexities that need careful consideration:

The RoI is structured as 15 interconnected spreadsheets, using common identifiers to link various data points. This design provides a detailed overview of all ICT dependencies.

The register must be maintained at the entity, sub-consolidated, and consolidated levels. It should also differentiate between ICT services that support critically important functions and those that do not. Additionally, the concept of the ICT service supply chain is crucial; the register should include details not only about direct service providers but also about subcontractors further down the supply chain.

The required reporting format for these submissions is plain CSV files, ensuring consistency and accessibility for regulatory review. ESMA has published an illustration of the register information template.

THANK YOU

Effectively managing the Dora Register of Information is essential for maintaining compliance and optimizing operations. At North House, we understand the complexities involved in handling such critical data. With our cutting-edge tool, we can help you stay on top of your information management needs.

Don't let data overwhelm you—get in touch with North House today to learn more about our solutions and how we can assist you in navigating the Dora Register of Information efficiently.

✉ dora@northhouse.se

☎ +46 8 502 352 22

🌐 www.northhouse.se