Published on *The National Law Review* https://natlawreview.com

Exploring DORA: Potential Implications for EU and UK Businesses

Article By:

Elizabeth (Liz) Harding

On Jan. 17, 2025, EU Regulation 2022/2554 on digital operational resilience for the financial sector (DORA) became applicable in the EU.

DORA focusses on risk management and resilience testing, with a strong focus on vendor risk management, incident management and reporting, and resilience testing of key systems.

DORA applies to financial institutions that are authorized to provide financial services in the EU and is designed to strengthen their IT security and operational resiliency.

It is worth noting, particularly for UK financial institutions, that DORA does not apply directly to organizations, including UK organizations, that are providing non-regulated services in the EU financial services industry. However, if a UK organization is providing any IT related services to an EU financial institution, it may be classified as an information and communication technology (ICT) third-party service provider under DORA. Depending on the nature of the organization and its services, it could be designated as a critical ICT third-party service provider, in which case it would have direct compliance obligations under DORA (which would include implementing a comprehensive governance and control framework to manage IT and operational resiliency risk).

As a high-level summary, financial institutions subject to DORA must:

- Create and maintain a register of vendors (ICT third-party service providers) and report relevant information from the register to financial authorities annually.
- Implement comprehensive security incident reporting obligations, requiring initial notification four hours after the incident is classified as major and a maximum of 24 hours after becoming aware. Follow-up obligations will also be required.
- Implement post ICT-related incident reviews after a major ICT-related incident disrupts core activities.
- Implement and maintain a sound, comprehensive, and well-documented ICT risk management framework, which must include appropriate audits.
- Establish and maintain a sound and comprehensive digital operational resilience testing program, which for critical functions must involve penetration testing.
- Clearly allocate, in writing, the financial entity’s rights and obligations when engaging with

ICT third-party service providers, including mandatory DORA contractual provisions.
- Adopt and maintain a strategy on ICT third-party risk.

As discussed above, ICT third-party service providers delivering services to financial entities will also be subject to DORA obligations. The nature of these obligations, and whether the ICT third-party service provider falls directly under DORA, will depend on various factors, including how critical the ICT service provider is to the EU financial services eco system, the nature of functions being supported, and services being provided. With that said, all ICT third-party service providers will be subject to contractual obligations resulting from the requirement for in-scope financial entities to flow down certain obligations to their service providers under DORA.

In light of the above, UK organizations providing services in the EU should carefully consider whether they fall directly under DORA in their capacity as a financial institution, and/or whether their services may cause them to be considered an ICT third-party service provider.

National Law Review, Volume XV, Number 57