Answers to your FAQs on the Digital Operational Resilience Act

07 August 2024

We are pleased to provide you with answers to a selection of frequently asked questions (FAQs) on the new Digital Operational Resilience Act (DORA) established by the European Union, which will be effective in January 2025.

What is DORA? What does it mean for the industry?

The Digital Operational Resilience Act (DORA) is a European Union (EU) regulation that aims to strengthen the technology security and resiliency of financial services, such as banks, insurance companies and investment firms, including a focus on third-party Information and Communication Technology (ICT) providers.

The key focus areas of the act are ICT Risk Management; Incident Management, Classification and Reporting; Operational Resilience Testing; Management of ICT Third-Party Risk; and Information Sharing Arrangements on Cyber Threats.

With the implementation of DORA, financial institutions must put into place a governance and control framework that enables the effective management of ICT risk as well as compliance with the rules for the protection from; prevention, detection of; response to and recovery from ICT-related incidents. DORA is specifically focused on ICT risk as a subset of operational risk and has detailed requirements with respect to on policies, procedures, controls and tools deployed by financial entities for managing ICT risks.

DORA will apply as of January 17, 2025.

What are the key regulatory requirements related to DORA?

The requirements are designed to enhance the operational resilience of the financial sector and enable it to better prevent, detect, respond to and recover from ICT-related disruptions, thereby enhancing the stability and security of the broader financial system in the EU.

We are committed to meeting DORA standards as they apply to the services that we provide to our clients.

The key regulatory requirements under DORA, also known as the 5 Pillars of DORA, are:

- **ICT Risk Management** — Establish and maintain a robust framework to identify, assess, mitigate, manage, monitor, and govern ICT risks
- **ICT-Related Incident Reporting** — Implement a process for classifying, and reporting major ICT-related incidents to authorities promptly and manage them effectively
- **Digital Operational Resilience Testing** — Regularly test ICT systems for their resilience, including conducting threat-led penetration tests
- **ICT Third-Party Risk Management** — Appropriately manage risks from third-party ICT service providers through due diligence, enhanced contracts, monitoring, inspections, and maintaining a detailed vendor register
- **Information and Intelligence Sharing** — Participate in arrangements to share cyber threat information and intelligence

Benefits of DORA

What are the main benefits of implementing DORA?

Implementing DORA is intended to enhance the industry's operational resilience, enabling financial entities to better respond to and recover from ICT-related disruptions. It also improves ICT risk management by promoting robust frameworks for better risk identification and mitigation.

DORA implementation aims to promote enhanced cybersecurity programs through regular testing, incident reporting and information sharing. It standardizes incident reporting for consistent and timely communication with authorities.

DORA also enforces greater accountability and governance by clearly defining roles and responsibilities for ICT risk management. It also enhances third-party risk management to manage the risks associated with external ICT service providers.

The regulation harmonizes standards across the EU, reducing regulatory fragmentation and creating a level playing field.

Overall, DORA encourages proactive threat management, and awareness of and responsibility for the resilience of ICT systems; thereby maintaining the stability and trust in the financial system.

State Street Planning and Readiness

What is State Street doing to meet the DORA requirements?

At State Street, we welcome the introduction of DORA as it enhances the industry's operational resilience with respect to IT incidents, an important priority for us and our clients. We are committed to meeting DORA standards as they apply to the services that we provide to our clients, and we are working to strengthen our operational resilience framework, recognizing that the landscape of digital threats evolves rapidly.

We have begun putting in progress the steps to comply with the new DORA regulation and are executing a detailed self-assessment and implementation program at a global level covering all subsidiaries, affiliates and functional lines of business.

Furthermore, we instituted a bespoke governance program and management oversight designed for the timely and effective implementation of DORA requirements. These steps will allow State Street to meet regulatory deadlines and enhance its digital operational resilience.

Who should I reach out to with questions regarding DORA?

Your first point of contact should always be your State Street representative.

Client Impact

How will this impact State Street's clients?

At this time, the regulators and the industry are still trying to assess and determine the path to compliance. It is an evolving process and the definition of ICT services subject to DORA requires additional clarifications that are expected from regulators. While we anticipate receiving clarifications to understand how DORA relates to the services that we provide to our clients prior to the effective date, we continue to work on our internal program to meet the requirements currently identified.

If you have questions, please reach out to your State Street representative.

Industry Reference Materials

Where can I find more detailed information on DORA?

Further information on DORA can be found in the below sources:

Official EU Publications — The official text of DORA can be found in the Official Journal of the European Union, which provides access to EU law and other public documents: Regulation - 2022/2554 - EN - DORA - EUR-Lex (europa.eu)

European Commission — The European Commission's website offers links to the implementing and delegated acts for DORA: Digital Operational Resilience Regulation - European Commission (europa.eu)

European Banking Authority (EBA) — The EBA provides guidelines, technical standards, and other resources related to the implementation of DORA: Digital Operational Resilience Act | European Banking Authority (europa.eu)

European Securities and Markets Authority (ESMA) — ESMA offers information on regulatory requirements and compliance related to DORA for securities markets: Digital Operational Resilience Act (DORA) (europa.eu)

These sources will provide comprehensive details on the regulatory requirements, implementation guidelines, and compliance strategies related to DORA.

We encourage you to review these important materials as they provide vital impact identification and transition preparation tools.