SPOTLIGHT ON THE DORA REGULATION

Strengthening Cybersecurity in the EU through Digital Operational Resilience

A Spotlight on the Implementation and Requirements of the Digital Operational Resilience Act (DORA)

StratisAdvisory

RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT

DORA Objectives, Coverage, and Legislation Timeline

The Digital Operational Resilience Act (DORA) was enacted in January 2023 and will take effect in January 2025, with the objective of incorporating the components of operational resilience in managing risk, strengthening the information technology security of banks, insurance companies and investment firms in the event of severe operational disruption. Before the introduction of DORA, financial institutions managed operational risk mainly through the allocation of capital. With the increasing dependence of financial institutions to technology and tech companies, the importance of managing risk involving information and communication technology (ICT) third-party service providers (TPSPs) has become more crucial than ever.

IMPLEMENTATION TIMELINES

2023

- **Jan** – DORA enactment
- **May to Jun** – Public consultation on the call for advice on criticality criteria and fees
- **Jun to Sep** – Public consultation on the first batch of policy products
- **End of Sep** – Call for advice on criticality criteria and fees

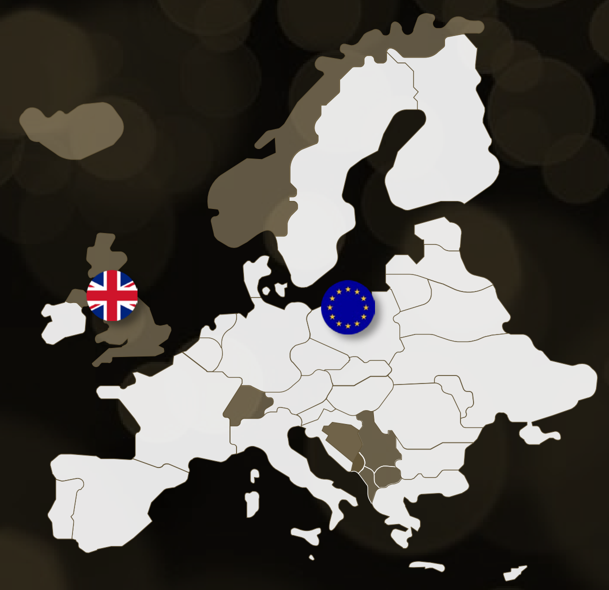
2024

- **Dec 2023 to Mar** – Public consultation on the second batch of policy products
- **Jan** – Delivery of First batch of policy products
- **Jul** – Delivery of the second batch of policy products

2025

- **Jan** 1 – DORA effective
- Start of the oversight activities for the European Supervisory Authority (ESAs) and Critical ICT Third Party Providers (CTPPs)

IMPACTED COUNTRIES



European Union (“EU”) Member Countries

EU Non-member Countries

REQUIREMENTS FOR FINANCIAL ENTITIES

DORA lays down uniform security requirements for network and information systems supporting financial entities' business processes on:

- ICT Risk Management
- ICT Third-party Risk Management
- Digital operational resilience testing
- ICT-related Serious Incident Reporting
- Information Sharing
- Oversight of Critical Third-party Providers

ICT AND OTHER REQUIREMENTS

DORA also requires financial entities to ensure that the following are established:

- Contractual agreements between service providers and financial entities.
- Rules to establish and conduct an Oversight Framework for critical ICT third-party service providers when providing services to financial entities.
- Rules on cooperation and supervision of competent authorities and enforcement to all matters covered by the Regulation.

FINAL DRAFT OF REGULATORY TECHNICAL STANDARDS ("RTS")

- ICT related incidents criteria for the classification and materiality thresholds for major incidents and significant cyber threats.
- Inclusion of contractual agreements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers to the policy.
- All contractual agreements on the use of ICT services provided by ICT third-party service providers will have standard templates for the purpose of the register of information.
- Reconciliation of ICT risk management tools, methods, processes and policies.

Discover what Stratis Advisory can do for you

Cybersecurity Risk Assessment

Beyond Service and Organization Controls (SOC) audit(s), penetration testing, and PCI Security Standard assessments, dedicated risk assessments help you understand the inherent risks in information technology systems, processes, and programs. Stratis can execute your cybersecurity risk assessment to identify broader risk identification and control mitigation across key information systems.

Third-Party Service Provider Assessment

A third-party service provider assessment is an evaluation used by organizations to assess risks and benefits associated with outsourcing to external entities. It ensures alignment with organizational policies, procedures, controls, cybersecurity, record keeping, and regulatory compliance. DORA codified operational resilience of third-party oversight, the UK has issued guidance on critical third parties (CTPs) and the US has routinely enhanced guidance on third party risk management. Stratis can help you develop, execute, and monitor third party risk management programs of vendors, including those identified as critical, to maintain domestic and international compliance with newly implemented laws and ongoing industry guidance.

Cybersecurity Program

Information systems documentation is typically disparate, involves multiple inputs from various third-party vendors performing a specific function, technically focused vs. operational execution, and fragmented without identified ownership across various functions. Stratis can consolidate your information systems and support your chief information security officer (CISO) with developing and maintaining a sustainable enterprise-wide cybersecurity program.

StratisAdvisory

LAUNCH | SCALE | OPTIMIZE

Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com