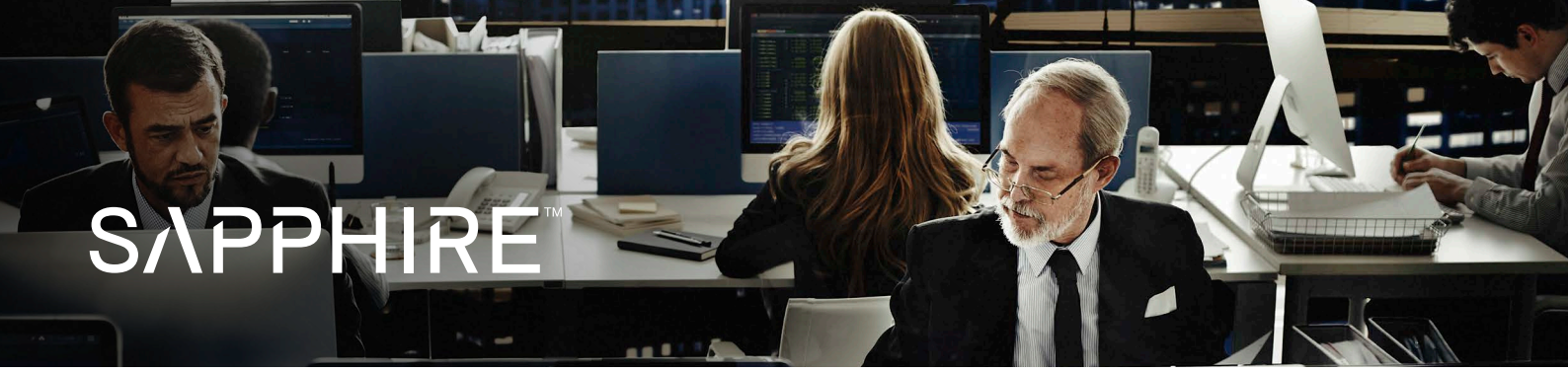

Digital Operations Resilience Act

Safeguarding your financial operations

The Digital Operations Resilience Act (DORA) is an EU regulatory framework designed to enhance the operational resilience of organisations within the financial sector. It provides a comprehensive approach to addressing the security challenges and risks posed by evolving threat landscapes in the financial sector, aiming to ensure that financial organisations have implemented the necessary safeguards to mitigate and respond to operational disruptions.

DORA is aligned with the wider EU Network and Information Systems (NIS2) regulations and is leading the way in relation to digital operational resilience for financial entities. All financial firms operating in Europe are required to comply with the Act. There is a global regulatory push towards operational resilience, and other regulation such as the Operational Resilience Act in the UK developed by the FCA, PRA and Bank of England, is expected to be aligned with DORA principles.

> DORA entered into force on the 16th Janaury 2023 and financial entities need to be complaint by 17th January 2025

The Digital Operational Resilience Act requires firms to consider resilience across their business with accountability at Senior Management level.

The Act focusses on five key areas to improve operational resilience:

- ICT Risk Management & Governance
- ICT related Incident Management
- Operational Resilience Testing
- Third Party Risk Management (TPRM)
- Information Sharing Arrangements

With mandatory compliance just round the corner, companies should be conducting Gap Analysis and developing their DORA security improvement plans before the January 2025 deadline.

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Understanding the impact of ICT disruptions relies on identifying Critical or Important Functions (CIFs) and mapping assets and dependencies to the CIFs. This should then be linked to a Business Impact Analysis based on severe business disruption scenarios.

Understanding the threats to the CIFs or their related assets and dependencies is instrumental in developing a robust Risk Management process.

Vulnerability Management and Penetration Testing are always the essential elements of any Risk Management process; however, DORA has taken this further with the introduction of Threat Led Penetration testing as a mandatory requirement.

DORA further strengthen the requirement for Third Party Risk Management, where the level of Supplier/Vendor assessment should be commensurate to the importance of the service offered, in relation to operational resilience.

Incident response planning, management and reporting must be documented and exercised for all Critical and Important Functions.

DORA introduces greater powers on digital operational resilience to National and EU Financial Supervisors, who are the regulatory authorities responsible for overseeing, regulating, and ensuring the stability and integrity of the financial systems within their jurisdiction. Different countries and regions have their own financial supervisory bodies.

Financial Supervisors responsibilities include but not limited to;

1. Ensuring financial entities have robust risk management process to identify, protect, detect, respond, and recover from ICT related incidents.
2. Overseeing the implementation of regular testing and audits to assess the effectiveness of the digital resilience controls.
3. Mandating the reporting of significant cyber incidents and ensuring effective responses to the incidents
4. Supervising the relationship between financial entities and their critical third-party service providers to manage supply chain risks.

Sapphire can assist with many of the DORA requirements, including but not limited to:

Service /Offering	Introductory	Foundations	Intermediate	Advanced
Prioritisation of CIF Suppliers	✓	✓	✓	✓
DORA Compliance Review	✓	✓	✓	✓
Gap Analysis	✓	✓	✓	✓
Security Improvement Planning	✓	✓	✓	✓
Security Awareness & Training	✓	✓	✓	✓
Procedure & Policy Review	✓	✓	✓	✓
DORA Compliance Audit		✓	✓	✓
Policy Development		✓	✓	✓
Risk Assessments		✓	✓	✓
Business Continuity Planning		✓	✓	✓
Business Impact Assessments of CIFs		✓	✓	✓
Incident Response Planning		✓	✓	✓
Threat Assessment		✓	✓	✓
Penetration Testing		✓	✓	✓
Threat Intelligence			✓	✓
Vulnerability Management			✓	✓
Development of Overarching Management System For Compliance			✓	✓
Third-Party Risk Management			✓	✓
Incident Response (24x7x365)			✓	✓
Identity & Access Management Review			✓	✓
Breach Attack Simulations (BAS)				✓
SIEM & SOC Advisory Services				✓
Endpoint Management (EDR/XDR)				✓
Breach Attack Simulation (BAS)				✓
Internal Audits				✓
Physical Security Audits				✓

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001