DORA

Digital Operational Resilience Act

EU Cyber Compliance Advisory

Overview

DORA aims to enhance digital resilience in the EU financial sector by introducing rigorous ICT risk management and testing requirements, which will be effective from January 17, 2025, for a wide range of financial institutions.

Targeted Business Sectors

- Credit Institutions
- Investment Firms
- Payment Institutions
- Electronic Money Institutions
- Insurance and Reinsurance Undertakings
- Central Securities Depositories
- Crypto-Asset Service Providers
- Trading Venues and Trade Repositories
- Account Information Service Providers
- Critical ICT providers (Cloud Services)

Challenges & Financial Impact

- Mandatory incident reporting to financial regulators, with a focus on root cause analysis and incident containment.
- Noncompliance can lead to significant penalties, including **daily fines of 1% of average daily global turnover** for up to six months.
- Noncompliance could lead to administrative sanctions, including the cessation of practices, financial sanctions, data transfer records access, and public notices of violations.
- Individual board members may face liability for failure to meet obligations under DORA.

How We Can Help

Security Monitoring (NSOC)

Continuous monitoring services can help financial entities detect and respond to ICT risks in real-time.

CSIRT

As DORA emphasizes incident reporting, having a dedicated CSIRT aligns with the directive's requirements.

Detection & Response (MDR/MPDR)

Support entities in incident detection and management processes, a core requirement of DORA.

Security Platforms Support & Management

Support the setup and management of ICT risk management platforms.

Vulnerability Scanning (VMS)

Help financial entities identify vulnerabilities, which is essential for maintaining ICT system security.

Governance, Risk, Compliance & Privacy (GRC-P)

Support entities with the management of third-party risk, especially around third-party ICT providers.

Threat Intelligence (TI)

Provide insights into potential cyber threats, allowing entities to be proactive in their risk management.

How Stefanini can Support DORA's 5 Pillars

ICT Risk Management

Stefanini can help your teams with identifying the main areas of risk, co-working with you to provide consistent evaluation End to End.

Managed Security Services
- Security Monitoring (NSOC)
- Detection & Response (MDR)
- Vulnerability Scanning (VMS)
- Threat Intelligence (TI)
- Security Platforms Support & Management

Advisory Services
- Governance, Risk, Compliance & Privacy (GRC-P)
- Regulatory Compliance
- Consultancy & Assessment Services

ICT Incident Reporting

By creating Processes and Playbooks for Incident Response, these can go hand in hand with Incident Reporting and Recovery.

Managed Security Services
- Security Monitoring (NSOC)
- Detection & Response (MDR)
- Phishing Detection & Response (MPDR)

Cyber Resilience Services
- CSIRT (Cyber Security Incident Response Team)

Digital Operational Resilience Testing

Customers will struggle both with skills and expertise, and the need to do rigorous independent testing. We can provide this in the following ways.

Cyber Resilience Services
- Ethical Hacking
- Penetration Testing
- Threat Hunting
- CSIRT (Cyber Security Incident Response Team)
- Security Platforms Support & Management

Advisory Services
- Consultancy & Assessment Services
- Technology Implementation Services

ICT Third-Party Risk Management

Third Party Supply Chain and Vendor Risks is a process going from recommendation to enforceable.

Advisory Services
- Regulatory Compliance
- Consultancy & Assessment Services (third-party risk assessments)

Cyber Resilience Services
- Penetration Testing

Information and Intelligence Sharing

While less of a core requirement, it is encouraged.

Managed Security Services
- Threat Intelligence (TI)

Advisory Services
- Security Awareness & Training

stefanini GROUP

HEADQUARTERS

EMEA - Brussels, Belgium
North America - Southfield, MI, USA
Global - Sao Paulo, Brazil
www.stefanini.com
info@stefanini.com