Delta Capita

Digital Operational Resilience Act

The European Response to Operational Resilience

Digital Operational Resilience Act: An Overview

Regulatory Engagement

- The Digital Operational Resilience Act comprises a key part of the Digital Finance Package, which sets out to "enable and support the potential of digital finance while mitigating the risks arising from it."
- DORAs purpose is to reduce the regulatory complexity around operational resilience by separating the requirements from those pertaining to operational risk, bringing them under a **single, operational resilience-focused framework**.
- DORA **overlaps significantly with many pre-existing EU policies**; both regional-specific Operational Resilience frameworks, and other risk management and business continuity related regulations.
- Firms will find they have already made significant progress in meeting many of DORAs requirements as part of their previous efforts to remain compliant with these various policies.
- By leveraging pre-existing processes and uplift practices that were implemented as part of these previous compliance projects, rather than duplicating their efforts will allow firms, firms can significantly reduce the cost of meeting DORAs requirements.

Who is Impacted

Despite applying to firms domiciled in the EU, non-European firms who engage in the European market fall under DORAs jurisdiction. Furthermore, whilst the regulation does not directly block the use of non-EU 3rd-party service providers, the provisions do complicate it for EU entities, restricting the outsourcing of critical ICT services to companies without European subsidiaries.

Key in-scope organisations include:

- Credit and payment institutions
- Trading venues and repositories
- Electronic Money Institutions
- Investment firms
- Crypto-asset issuers and service providers
- Central securities depositories
- AIF managers
- Insurance and reinsurance undertakings and intermediaries
- Institutions for occupational retirement pensions
- Securitisation repositories
- ICT 3rd-party service providers

Delta Capita Offering: SME-led Advisory and Compliance Readiness Services

We can support clients through several offerings ranging from an accelerated health check to end-to-end DORA compliance implementation. Our expert team is equipped with proprietary project accelerators and technology assets that adapt to our clients' requirements to further accelerate delivery speed and ensure client organisations are always ahead of the curve.

Accelerated DORA Health Check

Delta Capita SMEs will review your plan, perform a **quality assurance assessment** and benchmark the maturity of your overall program against industry best practice. In addition, the team will assess the existing, or proposed, BAU controls to ensure future adherence to the requirements. SMEs will put forward **recommendations to enhance current approach and highlight any gaps that might require remediation.**

Our Accelerators & Technology Assets

Self Assessment Checklist
'Ready to fill' self-assessment, board level, attestation templates for compliance evidencing

Critical Business Services & Impact Tolerances
Proprietary CBS scorecards and impact tolerance assessment templates to accelerate analysis

Asset Mapping & End-to-End Testing
Proprietary technology for end-to-end asset mapping & testing

Third Party Risk Management as a Service
An end-to-end Service that allows you to automate the monitoring of your 3rd, 4th and 5th party risks

DORA Compliance Readiness Services

GOVERNANCE DESIGN

We help our clients develop appropriate **firm-wide governance**, setting up suitable decision-making processes as well as defining and implementing **tailored risk and control frameworks**

ICT RISK MANAGEMENT FRAMEWORKS

With vast experience in establishing risk- management frameworks, our experts work with our clients to **manage, set up, and refine ICT frameworks** in line with DORA's risk requirements

ICT INCIDENT REPORTING FRAMEWORKS

Our team implement front-to-back **ICT incident management** frameworks, from governance to supporting tooling, as well as manage the **ICT incident monitoring** processes

DIGITAL OPERATIONAL RESILIENCE TESTING

Leveraging our expertise, we establish a resilience testing framework which includes **critical business services mapping**, **scenario definition** and **end-to-end testing**

ICT THIRD - PARTY TESTING

Our team conducts a quick **scan of the existing ICT 3rd-Party testing processes**, before setting up the necessary **Risk Taxonomy** tailored to our client's risk appetite and tolerances

INFORMATION SHARING ARRANGEMENTS

We install **information sharing procedures** governed by rules of conduct respecting business confidentiality and protection of personal data, as well as guidelines on competition policy