Global Cyber Risk Services

Thomas Murray

The Digital Operational Resilience Act

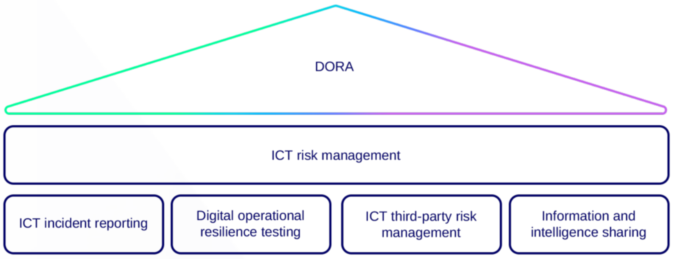
The EU's Digital Operational Resilience Act (DORA) addresses the risks posed by the digital transformation of financial services. It seeks to apply a consistent regulatory framework for digital operational resilience.

DORA will apply to more than 22,000 financial institutions and information communication technology (ICT) service providers based in the EU – including banks, investment companies, insurance companies and intermediaries, data reporting providers, and cloud service providers.

DORA non-compliance could lead to administrative fines, remedial measures to address any weaknesses or failures, public reprimands, withdrawal of authorisation, and orders for compensatory damages to clients, customers or third parties.

The pillars of DORA

Organisations are expected to meet the requirements set out in key areas by January 2025.


DORA

ICT risk management

ICT incident reporting

Digital operational resilience testing

ICT third-party risk management

Information and intelligence sharing

How we can help

Thomas Murray has developed a range of DORA compliance offerings that will enable your organisation to assess its current gaps.

We can provide you with a road map and detailed recommendations to achieving it through access to Thomas Murray's resources and cyber security experts. The breadth and extent of the team's experience means that we can provide clients with pragmatic, actionable advice that delivers lasting change, compliance and risk reduction.

Our two-step approach

Stream one: DORA gap analysis

Approach

Key TM activities:

- Initial questionnaire
- Interviews with stakeholders
- Documentation review
- Use of Orbit Security

Deliverables

- Summary: Executive report of current state
- Road map for compliance
- Actionable findings
- Recommendations
- Access to Orbit Security

Stream two: DORA compliance

Thomas Murray can provide the range of consulting support you need to establish the processes, procedures, and wider activities required for DORA compliance. How much help an organisation needs will be determined by the results of the gap analysis.

DORA readiness through Orbit Security: Based on the outcome of stream one, we design an action plan that is implemented through Orbit Security.

Oversee and manage: Programme management and oversight of an internal DORA compliance effort, with regular contact points and reviews of work by internal resources.

Enhance and optimise: Specified improvements in an existing controls framework through the execution of targeted programmes of work.

To find out more, contact:

William Rimington
Managing Director | Cyber Risk
wrimington@thomasmurray.com

Kevin Groves
Sales Director | Cyber Risk
kgroves@thomasmurray.com