# Digital Operational Resilience Act (DORA) Proposal

**10 March 2021**

EY
Building a better working world

**Mitigating the risks of digital transformation though common EU wide rules on digital operational resilience including ICT risk, testing, information sharing, ICT third party risk and incident reporting.**

## Why is DORA being introduced?

1

To mitigate the risk posed by growing vulnerabilities as a result of the increasing interconnectivity of the financial sector.

2

To address the increase in digitalisation which is changing the risk profile of organisations and the whole financial sector.

3

To acknowledge and address the third party reliance underpinning the stability of the financial sector.

4

To remediate the fragmented supervisory approach across the single market.

## DORA Operational Resilience Definition

The ability to build, assure and review operational integrity from a technological perspective by ensuring, either directly or indirectly, through the services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality.

## Key areas of DORA

### Background

The DORA proposal, published September 2020, forms part of the European Commission Digital Finance Strategy.

When the Act is implemented, it will be passed into law by each EU state. Further technical standards will be developed by the European Supervisory Authorities and compliance will be overseen by the existing National Competent Authority framework.

The Act will apply across the full financial sector, as well as to additional firms captured within the expanded regulatory perimeter under the term 'critical ICT third-party service providers', which will include services such as cloud resources, data analytics and audit.

The final regulations are expected to be published towards the end of 2022, with date of compliance and additional technical standards 12-18 months later.

*It should be noted that the Act is currently in draft; it is expected that there will be changes in the final publication.*

### ICT Risk Management Framework and Governance

Builds largely on the EBAs ICT and Security Risk guidelines, defining how to manage risks through each stage of their lifecycle, emphasising the role of senior management and expanding the requirements to include a digital resilience strategy. There are also additional requirements around disaster recovery, communications and crisis management. The proposal also sets out requirements to learn and evolve both from external events as well as the firm's own ICT incidents.

### Incident Reporting and Information sharing

Expands the reporting of ICT related incidents to sectors not currently covered. It also addresses the multitude of reporting requirements imposed on a firm, and attempts to streamline reporting with common reporting templates, timeframes and single point of reporting. Additionally, the guidelines encourage the exchange of cyber threat information and intelligence within trusted communities of other financial entities.

### Management of ICT Third Party Risk

Builds on existing EBA Outsourcing requirements, requiring firms to expand their register of providers to include all contractual arrangements rather than just those classified as outsourcing. DORA also requires firms to have a strategy on ICT third party risk. It sets out more detailed guidance around the content of exit plans and substitutability assessments as well as requirements to test them. The regulations also look to limit the use of third parties outside of the EU.

### Operational Resilience Testing

Suggests that firms should establish proportionate testing programs to their size, business and risk profiles which include a range of assessments, tests, methodologies, practices and tools. Ultimately, testing should be risk-based and take into account the risk horizon, as well as firm-specific risks and the criticality of ICT resources and the services that they support. Testing should consider the principle of applying 'extreme scenarios' where relevant and involve participation of contracted third parties.

## Next steps

Financial Institutions currently under the European Commission's supervisory model and scope should assess if their current state meets the expanded regulation and plan accordingly to respond across the themes.

## Digital Operational Resilience: Suggested considerations

### ICT risk framework

Assess your existing ICT risk strategy, policies, procedures and tools. Consider roles and responsibilities as well as skills in IT and Risk.

### Testing – 'basic'

Review the scope and coverage of what would constitute your 'digital operational resilience testing' program against DORA articles.

### Testing – 'advanced'

Continue to assess the scope of threat-led penetration testing (akin to CBEST and TIBER), which contributes to DORA testing expectations.

### 'Critical' ICT third party status

Assess the services received from third party service providers to identify any that would be captured and require an additional level of governance and oversight

### Governance

Assess your existing ICT risk governance (for regulated entities, and inter-entity) to identify gaps in direction, evaluation or monitoring of ICT risk topics.

### Incident reporting

Review your incident identification, classification and reporting protocols against leading practice to identify where you may need to invest in process/tooling.

## Client experience

We have a track record of delivering operational resilience transformation. We continue to evolve our thinking and delivery approaches as the industry regulatory environment and nature of resilience challenges evolve.

## Contacts

**Jerry O'Sullivan**
Associate Partner
jerry.osullivan@ie.ey.com

**Sara Woods**
Senior Manager
sara.woods@ie.ey.com

## How EY can help

### Current state assessments of resilience capability and building a multi-year roadmap

Perform assessment by leveraging existing mapping information (such as business impact analysis, privacy data flow mapping, technology asset inventories) that exist within the organisation.

### Testing clients' ability to meet impact tolerances

Test impact tolerances at the appropriate level for the organisation and the service – incorporating different impacts caused by disruption to different products, legal entities or locations, through a severe but plausible event.

### Mapping clients' end-to-end important business services and setting impact tolerances

Identifying important business services, to ensure resilience capability is proportionate, helps in differentiating which areas need resilience measures due to the harm that their outage could cause.

### Setting resilience dashboards and reporting for senior stakeholders

Dashboards and reporting to key stakeholders should be actionable and understandable, and include information on significant initiatives, investments, regulatory focus areas and emerging risk themes.

**EY** | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.



131403.pptx. Produced by Creative (Ireland). 03/2021. ED none.



Ernst & Young, Harcourt Centre, Harcourt Street, Dublin 2, Ireland.



**ey.com**