Digital Operational Resilience Act (DORA) Proposal

Mitigating digital transformation risk though common EU-wide rules on operational resilience

Why is DORA being introduced?

1. To mitigate risk posed by growing vulnerabilities, due to the increasing interconnectivity of the financial sector
2. To address the shift in risk profile as a result of the increase of financial services digital adoption
3. To acknowledge and address the third party reliance underpinning the stability of the financial sector
4. To adopt a single, consistent supervisory approach to operational resilience across the single market

Operational Resilience is the ability to build, assure & 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, & which support the continued provision of financial services & their quality.

EY
Building a better working world

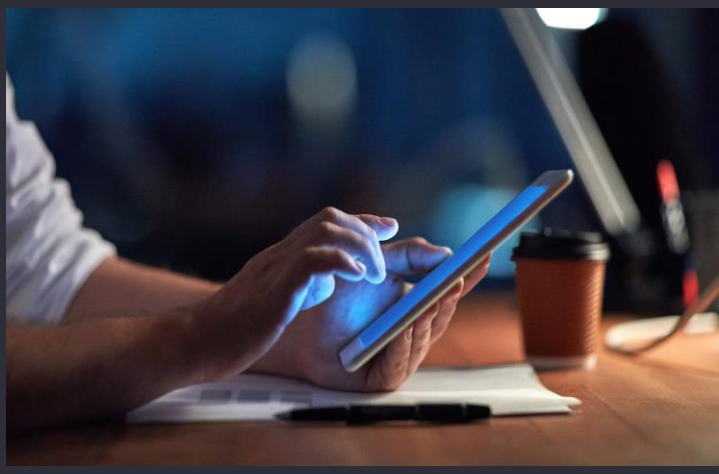
Key areas of DORA

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

DORA scope and rollout

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.

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, it attempts to streamline reporting with common templates, timeframes and single point of reporting. Additionally, the guidelines encourage collaboration among trusted communities of other financial entities on cyber threat information and intelligence.

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 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

Suggest that firms should establish testing programs proportionate 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.

Suggested considerations

ICT risk framework

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

Testing – 'basic'

Review the scope and coverage of what would constitute '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 an additional level of governance and oversight

Governance

Assess 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 incident identification, classification and reporting protocols against leading practice (including existing PSD2 expectations) to identify if investment in process/tooling is needed.

EY operational resilience service offerings

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.

Understanding clients' critical end-to-end business services, mapping and setting impact tolerances for each of them

Identify 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 stakeholder should be actionable and understandable, and include information on significant initiatives, investments, regulatory focus areas and emerging risk themes.

Profiling third parties and assessing their risk and controls leveraging your technology and framework or ours

Service risk profiling and perform global onsite and remote-control assessment execution across all risk domains (e.g. resiliency, cyber, financial health and regulatory compliance)

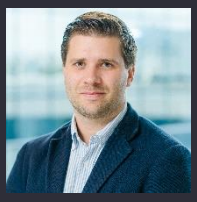
Contacts

To find out how the EY Financial Services Technology Risk team can support you, please contact a member of the team.

Sylvie Goethals

Partner
EY Consulting

sylvie.Ggoethals@be.ey.com



Robin Blondeel

Senior Manager
EY Consulting

robin.blondeel@be.ey.com

EY | Assurance | Tax | Transactions | Consulting

About EY
EY is a global leader in assurance, tax, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

1811-2964932
ED None

ey.com