OliverWyman

Thomas Ivell
Mark James
Miriam

Against this backdrop, the European Council has set an intention to bring stricter guidance and oversight on how ICT risks are managed, acknowledging that there is a proliferation of both national and international regulatory initiatives and supervisory approaches. Given the ever-increasing risks of cyberattacks and the importance of a resilient financial sector, the Commission aims to develop an approach that fosters technological development and ensures financial stability and consumer protection.

To this effect, it has set out to define a detailed and comprehensive framework on management of ICT risks for EU financial entities, the Digital Operational Resilience Act (DORA), which was adopted by the European Council in November 2022 and is now being

The level of detail in the regulation varies across different pillars. Some elements of the regulation are highly prescriptive, for example listing exact elements the regulator thinks should be included in an ICT third-party provider contract. Other parts are comparatively high level, such as the guidance on what should be included in the governance and control framework.

We expect DORA to be an evolving standard that will change as operational resilience practices develop and standards are iterated between regulators and industry. What is clear, however, is that operational resilience is increasingly looking to become a prime focus of regulators this decade.

Complying with DORA won't be easy. For many organizations the regulation fundamentally changes how operational resilience is currently thought about, requiring institutions to deconstruct and assess the complexity of their own IT systems and processes and answer some tough questions on their management of ICT risk for critical business services.

Based on the emerging guidance across the five pillars, there are a number of key requirements we observe that introduce challenges for institutions in building resilience, while also posing a number of questions on the practicalities of implementation for institutions (see table on following page).

Fundamentally, instilling operational resilience throughout the organization requires a deliberate approach driven top-down by senior management and the board, who will need to be involved in defining the operational resilience strategy and how it links to the business strategy.

Financial entities should already start undertaking measures to prepare for DORA. The length of time required to enact the required standards across the entire organization, including all underlying entities, should not be underestimated due to the need to engage a diverse set of stakeholders, secure sufficient investment to implement the necessary capabilities, and balance the implementation alongside what is an already busy portfolio of technology work.

The long-term competitive benefits of better operational resilience are undeniable — complying with the spirit of DORA as opposed to approaching it as a 'box-ticking exercise' — will yield significant upside. Fundamentally, DORA presents organizations with a pivotal opportunity to strategically redesign their framework for management of technology-related risks and build end-to-end resilience throughout the enterprise. Improving operational resilience will have

Summary requirements

- the data losses.
- the severity of the impact of the ICT-related incident on the financial entity's ICT systems.
- the criticality of the services affected.
- the economic impact of the ICT-related incident.

- Financial entities shall report major ICT-related incidents to the relevant competent authority within tight time-limits. Financial entities shall produce, after collecting and analyzing all relevant information, an incident report and submit it to the competent authority.
- Fio ⅔] ᵐ M] t ł ll í et or À

	Pillar	Summary requirements
4	**ICT third-party risk**	• Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework and in accordance with key principles for ICT third party risk management issued by the regulatory authority. • Financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall at all times remain fully responsible for complying with, and the discharge of, all obligations under this regulation and applicable financial services legislation. • The management of ICT third-party risk shall be implemented [illegible]

Oliver Wyman is a global leader in management consulting. With offices in more than 70 cities across 30 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm has more than 6,000 professionals around the world who work with clients to optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities.

For more information, please contact the marketing department by phone at one of the following locations:

Americas	EMEA	Asia Pacific
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700