OliverWyman

PREPARING FOR THE NEW DIGITAL OPERATIONAL RESILIENCE RULES

Are financial institutions ready?

Thomas Ivell
Mark James
Miriam Martin
Nikita Nikitin

EXECUTIVE SUMMARY

Rapid digitization of the European financial services sector in the last two decades has put technology at the center of all financial activities, exposing institutions to a broad set of new and emerging risks. In response, institutions have built out controls aimed at mitigating these risks and have developed back-up protocols to "keep the lights on" in the event that critical digital infrastructure fails.

But maintaining robust defenses against information and communications technology (ICT) risks has not come naturally to many financial institutions. Efforts to establish operational resilience often have been haphazard and poorly coordinated, resulting in deficient control environments or poor backup plans for critical activities. Making matters worse, board members and senior managers are often unaware that the institution is running unacceptably high levels of ICT risk because management information is poor or non-existent. A series of high-profile outages and business disruptions at European banks over the last few years has underscored the threat that the lack of operational resilience poses for the industry.

In response, the European Council has turned its attention to instilling more robust operational resilience across the financial services sector, while consolidating and harmonizing existing national regulation.

The Digital Operational Resilience Act (DORA) sets out a detailed and comprehensive framework for the management of ICT risks for European financial institutions.

DORA consists of five pillars that lay out requirements and expectations for different aspects of operational resilience: ICT risk management and governance, ICT-related incident reporting, digital operational resilience testing, ICT third-party risk, and information sharing.

While DORA is still an evolving standard, the direction of travel from the regulator is clear and requires a fundamental mindset shift across institutions.

Complying with DORA will not be easy — it requires a purposeful and deliberate business-led technology strategy, and an integrated risk management approach aligned to critical business services.

The size of the prize from better operational resilience is potentially enormous: reduced financial losses from operational incidents, faster and more trouble-free implementation of new systems, maintenance of good customer service levels, increased brand value, lower risk management costs, as well as lower regulatory risk. Building digital operational resilience is not optional and no longer a topic that is confined to specialists in IT and risk; it needs widespread engagement from across the organization, including from individual business lines, senior management, and boards.

THE CASE FOR OPERATIONAL RESILIENCE

In the last two decades financial institutions have grown rapidly, driven by large investments in technology and increasing digitization of processes. With more than 80% of payments in the European Union being processed electronically, according to a study by industry group Payments Europe, and the volume of data stored in the cloud by banks expected to double over the next three years according to another recent study, the industry is seeing the level of digitization reach new peaks. Financial institutions have become increasingly exposed to a wide spectrum of digital-related risks — everything from fraud and malicious attacks to technical outages and data losses. In response to these emerging risks, financial institutions have been on a journey to build controls that establish operational resilience — the ability to prevent, respond, recover, and learn from operational disruption.

Efforts to build operational resilience have been fragmented and inconsistent within financial institutions. Typically, IT teams have looked after operational resilience in a silo, putting in place controls and backup plans for new digital assets in order to maintain operational continuity. Security teams under the chief information security officer may put in place further controls aimed at managing cyber risk. Risk teams have focused on ensuring there are appropriate second-line controls and oversight, yet often at a less operational level. Business leaders often neglect giving adequate focus to the control environment, assuming the responsibility of implementing and operating controls sits with the IT, security, and risk teams. Meanwhile compliance is predominantly focused on force-fitting these activities and controls to align with what the regulator has demanded.

With so much activity taking place in silos, there has been a fundamental lack of a joined-up, integrated approach.

Recent well-publicized incidents in Europe, such as failed bank IT migrations that led to millions of customers being unable to access online services and trading stops after serious technical failures impacted exchanges' data management systems, have demonstrated that the threat of operational incidents is real. With operational disruptions and a rapidly evolving threat landscape becoming increasingly prevalent, the European Council's focus has turned to getting a tighter grip on operational resilience across the financial services sector.

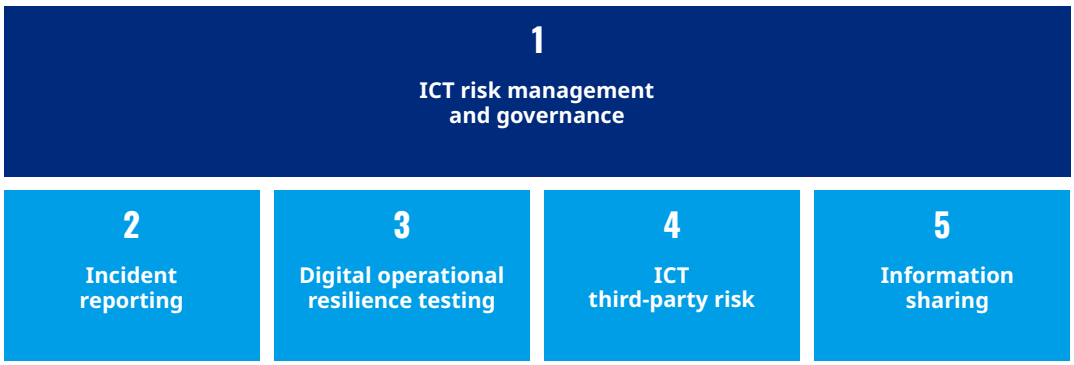
INTRODUCING 'DORA'

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 transposed into law by each EU member state, with an expected two-year implementation period. The regulation applies to a wide array of financial entities, from traditional financial services players such as credit institutions, payment institutions, investment firms, and exchanges, to more recent entrants to the sector such as crypto-asset services, fintechs, and ICT third-party providers.

DORA goes beyond existing regulations by bringing together multiple aspects of operational resilience into one framework, while also increasing the level of expectations on how institutions go about managing ICT risks. It sets out a broad set of requirements across five foundational pillars shown in Exhibit 1.

Exhibit 1: Five pillars of DORA



The approach centers on identifying critical business services and building the resilience framework around them. This reflects a mindset shift by the European regulator and an evolution to approaches observed at the Federal Reserve and Bank of England, in which the strategy for building resilience is more outcomes-based.

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.

THE CHALLENGE OF DORA COMPLIANCE

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.

Exhibit 2: Challenges and questions raised by DORA

Pillar	Summary requirements	Challenges observed	Key questions for Financial Institutions
1 ICT risk management and governance	The management body of a financial entity is required to define, approve, oversee, and be accountable for the implementation of all arrangements related to the ICT risk management framework	• Senior management and board-level accountability is expected, which should link the business strategy to the resilience strategy • An integrated risk management approach is required that designates and agrees across the enterprise what the critical business services are and which assets are instrumental in driving those	• What is the exact role of senior management and the board in steering the digital resilience strategy? • How to achieve business benefits from end-to-end management of critical business services? • What are the organizational implications of this framework? • Where do we start?
2 ICT-related incident reporting	Financial entities are required to establish and implement an ICT-related incident management process to detect, manage, and notify ICT-related incidents and shall put in place early warning indicators as alerts	• Integration of predictive analytics into incident management through early warning indicators is necessary to drive proactivity in the organization • A classification framework for incident handling should guide proportionality and consistency in the response	• What set of early warning indicators should be monitored? • How can incident management and reporting be made consistent despite differing national reporting requirements? • How should severity thresholds be set for classifying ICT-related incidents?
3 Digital operational resilience testing	Financial entities are required to establish and implement an ICT-related incident management process to detect, manage, and notify ICT-related incidents and shall put in place early warning indicators as alerts	• A comprehensive testing program should be in place that considers a wide variety of tests limited not just to IT systems, but also extending to processes and people • The overarching testing regimen should be governed through a risk-based approach, taking into account service criticality	• How can existing testing programs be adapted to meet these requirements? • Which kinds of tests should be used for which systems and applications? • Which tests can be performed internally and which require independent external testers?
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	• A purposeful and deliberate business-led strategy for use and management of third-party providers is required • Adequate due diligence of third party providers with contractual agreements that clearly set out rights and obligations	• Is the overarching ICT third-party risk strategy clearly purposeful and deliberate? • Is the cost of risk management for smaller, less sophisticated third-party vendors worth it?
5 Information sharing	Financial entities may exchange among themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts, and configuration tools	• Organizations should be on the front foot in exchanging cyber threat information and intelligence, with it being better to have something already in place than waiting for the regulator to introduce clear standards and templates	• Which entities should be in charge of setting up and running the information exchange alliances? • How should sensitive technical information be shared to the benefit of all? • What tooling is required to facilitate information sharing?

Note: Detailed requirements for each pillar can be found in the Appendix.

BENEFITS OF A MORE RESILIENT INSTITUTION

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 repercussions broadly, from improving client experience, allowing employees to perform their roles more effectively, to reducing the financial losses associated with operational incidents.

Exhibit 3: Benefits of operational resilience

Improved client experience

Streamlined customer experience and improved customer service levels with less disruption

Increased Brand Value

Strengthened brand reputation and value

Reduced Financial Losses

Lower direct costs associated with critical incidents such as client compensation or regulatory fines

Effecient Implentation

Seamless implementation of new systems with an integrated risk strategy

Lower Risk Managment Costs

Fewer high-risk events and a more streamlined risk management process result in lower costs

Lower Regulatory Risk

Reduced risk of regulatory non-compliance with international or regional legislation

In light of these benefits, senior management and boards should be driving operational resilience as a key agenda item, with active involvement from key stakeholders across the organization. Building operational resilience for financial institutions is not optional and no longer a topic that is confined to specialists in risk and IT.

APPENDIX: DORA REQUIREMENTS BY PILLAR

Pillar	Summary requirements
1 ICT risk management and governance	• Financial entities shall have in place internal governance and control frameworks that ensure an effective and prudent management of all ICT risks. • Financial entities shall have a sound, comprehensive, and well-documented ICT risk management framework, which enables them to address ICT risk quickly, efficiently, and comprehensively and to ensure a high level of digital operational resilience that matches their business needs, size, and complexity. • Financial entities shall use and maintain updated ICT systems, protocols, and tools. • Financial entities shall identify, classify, and adequately document all ICT-related business functions, the information assets supporting these functions, and the ICT system configurations and interconnections with internal and external ICT systems. Financial entities shall review as needed, and at least yearly, the adequacy of the classification of the information assets and of any relevant documentation. • For the purposes of adequately protecting the ICT systems and with a view to organizing response measures, financial entities shall continuously monitor and control the functioning of the ICT systems and tools and shall minimize the impact of such risks through the deployment of appropriate ICT security tools, policies, and procedures. • Financial entities shall have in place mechanisms to promptly detect anomalous activities, including ICT network performance issues and ICT-related incidents, and to identify all potential material single points of failure. • Financial entities shall put in place a dedicated and comprehensive ICT business continuity policy as an integral part of the operational business continuity policy of the financial entity. • For the purpose of ensuring the restoration of ICT systems with minimum downtime and limited disruption, as part of their ICT risk management framework, financial entities shall develop a backup policy and recovery methods. • Financial entities shall have in place capabilities and staff, suited to their size, business, and risk profiles, to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyberattacks, and analyze their likely impacts on their digital operational resilience.
2 ICT-related incident reporting	• Financial entities shall establish and implement an ICT-related incident management process to detect, manage, and notify ICT-related incidents and shall put in place early warning indicators as alerts. • Financial entities shall establish appropriate processes to ensure a consistent and integrated monitoring, handling, and follow-up of ICT-related incidents, to make sure that root causes are identified and eradicated to prevent the occurrence of such incidents. • Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria: – the number of users or financial counterparts affected by the disruption. – the duration of the ICT-related incident. – the geographical spread.

		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. • Upon receipt of a report, the competent authority shall acknowledge receipt of notification and shall as quickly as possible provide all necessary feedback or guidance to the financial entity, to discuss remedies at the level of the entity or ways to minimize adverse impact across sectors.
3	**Digital operational resilience testing**	• For the purpose of assessing preparedness for ICT-related incidents, of identifying weaknesses, deficiencies, or gaps in the digital operational resilience and of promptly implementing corrective measures, financial entities shall establish, maintain, and review, with due consideration to their size, business, and risk profiles, a sound and comprehensive digital operational resilience testing program as an integral part of the ICT risk management framework. – Financial entities shall follow a risk-based approach when conducting the digital operational resilience testing program and shall test all critical ICT systems and applications at least yearly. • The digital operational resilience testing program shall provide for the execution of a full range of appropriate tests. – Including vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing, or penetration testing. • Threat-led penetration testing shall cover at least the critical functions and services of a financial entity and shall be performed on live production systems supporting such functions. – Financial entities shall carry out at least every three years advanced testing by means of threat led penetration testing. • Financial entities shall ensure that tests are undertaken by independent parties, whether internal or external. Financial entities shall only use testers for the deployment of threat led penetration testing, which: – are of the highest suitability and reputability. – possess technical and organizational capabilities and demonstrate specific expertise. – are certified by an accreditation body in a member state or adhere to formal codes of conduct or ethical frameworks. – in case of external testers, provide an independent assurance or an audit report in relation to the sound management of risks associated with the execution of threat led penetration testing. – in case of external testers, are dully and fully covered by relevant professional indemnity insurances.

	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 in light of the principle of proportionality, taking into account the scale, complexity, and importance of ICT-related dependencies, and the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers. • When performing the identification and assessment of ICT concentration risk, financial entities shall take into account whether the conclusion of a contractual arrangement in relation to the ICT services would lead to any of the following: contracting with an ICT third-party service provider that is not easily substitutable or having in place multiple contractual arrangements in relation to the provision of ICT services with the same ICT third-party service provider or with closely connected ICT third-party service providers. • The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in a writing. The full contract, which includes the services level agreements, shall be documented in one written document available to the parties on paper or in a downloadable and accessible format. It encompasses at least the set of minimum requirements given in DORA Article 27.
5	**Information sharing**	• Financial entities may exchange among themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts, and configuration tools, to the extent that such information and intelligence sharing: – aims at enhancing the digital operational resilience of financial entities, through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting financial entities' range of defensive capabilities, threat detection techniques, mitigation strategies, or response and recovery stages. – takes places within trusted communities of financial entities. – is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data, and guidelines on competition policy.

GET IN TOUCH

Oliver Wyman specializes in financial services and brings an agile, cross-functional approach, connecting our experts across our Risk, Performance Transformation, and Digital practices to help financial institutions get on top of such complex, multidisciplinary issues. We are already working with a number of leading European financial institutions on DORA preparedness and are in discussions with regulators across Europe on implementation considerations for when the regulation comes into force.

We would be happy to share further perspectives on the impacts of DORA and how to build operational resilience within your organization.

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

AUTHORS

Thomas Ivell
Partner, Finance & Risk
thomas.ivell@oliverwyman.com

Miriam Martin
Partner, Finance & Risk
miriam.martin@oliverwyman.com

Mark James
Partner, Digital
mark.james@oliverwyman.com

Nikita Nikitin
Principal, Digital
nikita.nikitin@oliverwyman.com