DIGITAL OPERATIONAL AND CYBER-RESILIENCE

MARGARITA DELGADO
Deputy Governor - Banco de España

Challenges for a coordinated and proportional approach to resilience

While the financial sector has always been keen to adopt new technological solutions to improve the services it offers and increase efficiency, the current speed of digital transformation at financial institutions is unprecedented. Changing customer expectations, greater competition within the sector (together with new actors offering financial services) and the pace of technological development have significantly accelerated this transformation.

Increased digitalization also entails greater ICT (information and communication technology) and cyber risks. Not only are malicious attacks against financial institutions and their customers on the rise, the huge complexity of such institutions' ICT systems also makes operational mistakes more likely. Additionally, institutions' increasing reliance on specialized third parties, very often involving a multi-level supply chain, makes operational risk management an even more challenging affair.

With the goal of supporting digital transformation in the financial sector, while ensuring an adequate level of operational resilience, the EU has published DORA[1] and the NIS2[2] Directive, two different but complementary regulatory approaches to the problem. While DORA is a common text applicable to the entire EU financial sector, NIS2 is a transversal directive focused on the cybersecurity of the most critical sectors in each jurisdiction, including the financial sector. Not surprisingly, both texts set out supervisory frameworks for some critical technology service providers, showing a clear determination on the part of the EU to address the issue of dependency on these third parties. The coexistence of the two supervisory frameworks will require close coordination between the DORA and NIS2 authorities.

The requirements applicable to financial institutions need to be proportional to their specificities.

But this is not the only issue that will need to be clarified in the Level 2 regulatory standards. The requirements applicable to financial institutions as regards ICT risk management, ICT-related incident classification and reporting, resilience testing and third-party risk management must be proportional to the size and overall risk profile of such institutions and the nature, scale and complexity of their services, activities and operations. Easy to say, but extremely hard to define in a legal text, striking the right balance between prescriptiveness and legal certainty, on the one hand, and a principles-based, technology-neutral and future-proofing approach on the other.

The precise structure of relations between the DORA and NIS2 ecosystems will also need further clarification, on aspects such as how information on significant incidents and threats is to be shared or the role of the NIS2 authorities in the DORA mechanism for oversight of critical ICT third parties.

Due to its innovative nature, this mechanism is, by far, the section of DORA that has attracted the most attention. While defining the detailed governance arrangements required to set up the oversight system in the Level 2 texts will no doubt be challenging, actual implementation will be doubly so. This is in part due to a complex decision-making process in which the ESAs[3], the competent authorities and observers such as the European Central Bank, the European Single Resolution Board, the European Agency for Cybersecurity (ENISA) and the NIS2 authorities are all involved. Moreover, practical aspects such as the identification of the most critical ICT third parties or how to ensure that examination teams are sufficiently staffed with skilled personnel are still under discussion.

It is fair to highlight the additional challenges that both regulations pose for the authorities in terms of resources and cooperation. Building the necessary capacity and learning to work together at this scale will require a major effort on all our parts.

Financial institutions also have gaps to fill, with significant differences across entities as regards their levels of readiness and awareness. Although the precise requirements will only be clear once the Level 2 work has been completed, there is already enough detail in the legal texts to start working in the right direction. NIS2 will be applicable as from October 2024, and DORA as from January 2025.

Financial institutions, authorities and providers must continue working hard to meet these tight deadlines and contribute to the common goal of enhancing the EU financial sector's operational resilience.

[1] Digital Operational Resilience Act
[2] Directive on measures for a high common level of cybersecurity across the Union
[3] European Supervisory Agencies, namely EBA, ESMA and EIOPA

GERRY CROSS
Director Financial Regulation – Policy and Risk -
Central Bank of Ireland

DORA - A truly cross-sector ICT Regulation

DORA is a cross-sector Regulation, affecting all regulated financial firms. It has the key objective to mitigate technology and cyber risk by enhancing the ability of financial firms to build and ensure on an ongoing basis their operational integrity and resilience. The European Supervisory Authorities (ESAs) are tasked with jointly delivering the regulatory standards implementing the framework. The Joint Committee of the three ESAs has established a Sub-Committee to deliver these standards.

DORA will change the way regulated firms and supervisory authorities look at ICT risk. A key to overcome challenges will be early stakeholder engagement. The ESAs jointly started such engagement earlier this year with a technical event on the Digital Operational Resilience Act attended by more than 2000 interested parties. Events like this, including the upcoming public consultations for the Level 2 regulatory standards, will be important in delivering a high quality final framework.

The financial sector has always relied heavily on ICT and the COVID-19 pandemic has further intensified reliance on remote working and on network connectivity as well as ICT infrastructures to support it in a secure manner. The consequences of a cyber-attack or disruption of an important cross-border financial service can have far-reaching effects on other companies, sub-sectors, or even the rest of the economy.

DORA's relevance in mitigating these risks across all member states and across all sectors is clear but not without challenges given its ambition in setting expectations across the whole spectrum of ICT risks.

ICT risk management principles are not different to operational risk management, but complexity derives from the requirement that firms have a good understanding of all their ICT assets and their respective vulnerabilities. DORA will require regulated financial firms to identify, classify and adequately document all ICT supported business functions and to identify, classify and adequately document all the information assets and ICT assets supporting these functions. This will be a challenge for some firms, especially those with complex ICT systems or extensive reliance on outsourced ICT services.

DORA's operational resilience testing requirement will bring significant benefits but also implementation challenges.

DORA is a cross-sector regulation, affecting all regulated financial firms.

DORA Level 2 regulatory standards will provide templates for the creation of a register of information for all contractual arrangements regarding ICT services provided by third-party providers and for the reporting of ICT incidents. Harmonizing ICT incident reporting will be challenging because of the number of different ICT incident report recipients and on the other hand the need for a timely notification of incidents. In addition, two other EU directives, NIS2 and the Critical Entities Resilience Directive (CER), are being introduced to strengthen the resilience of European infrastructure, with DORA intended to operate as lex specialis for both for the financial sector.

The new oversight framework and the designation of critical third-party providers (CTPP) is new territory for both regulators and technology firms and will bring new challenges. Level 2 regulatory standards are currently being developed to establish oversight frameworks and designation criteria.

SAMU KURRI

Head of Department - Finnish Financial Supervisory Authority (FIN-FSA)

An entirely new role for financial supervisors

With the high degree of digitalisation of the financial sector, it is utmost important to prepare for various cyber threats. The cyber resilience of the financial sector is generally at a good level thanks to long tradition in risk management. Already today, several regulations oblige financial entities to ensure an adequate level of information management, information security and business continuity. Supervisors, like the FIN-FSA, monitor the fulfilment of these requirements during new entities' authorisation and registration phase, through inspection activities and other supervisory duties. Supervisors also monitor significant disruptions in the services provided by the financial entities as well as in payment and information systems.

DORA brings an important step towards an even stronger harmonization of the supervision of ICT and cyber threats in the EU. NIS2, on the other hand, ensures that the important pipeline, including electric and information networks, that is required for providing digital financial services, is resilient for cyber threats.

Already for some time, supervisors have been witnessing the growing number of outsourcing notifications from financial entities. DORA introduces an entirely new role for financial supervisors. For now, financial sector supervisors have been the watchdog for financial sector entities. DORA brings critical ICT third-party service providers of the financial sector under their supervision.

The Lead Overseer that is appointed among the ESAs conducts oversight of the critical ICT third party service providers. Joint examination teams that consist of staff from ESAs and national competent authorities assist the Lead Overseer in particular in investigations and inspections.

This entirely new role requires extensive preparation, but it is a necessity considering the fast pace of outsourcing activities. We need clear processes for both ongoing and periodic supervision of the critical third-party ICT providers to succeed. This new role also puts supervisors´ credibility to test. Supervision must be structured so that there are no loopholes. Joint examination teams that assist the Lead Overseer need to function effectively from early on.

An important step towards an even stronger harmonization of the supervision of ICT and cyber threats.

The has often been very little or no room for negotiation with the large and critical ICT third-party providers. DORA introduces requirements for the key contractual provisions and defines the elements that should at least be included in the contractual arrangements on the use of ICT. The key contractual provisions shall contain clauses on exit strategies, in particular the establishment of a mandatory adequate transition period. In practice, the switching of ICT third-party provider may be impossible.

The degree of concentration in ICT outsourcing among financial entities is an element that needs further scrutinization also after the application of DORA. The FIN-FSA has witnessed the names of certain ICT services providers popping out in the outsourcing notification documents more frequently than others. This raises concentration risks that should be further observed from systemic point of view.

Finally, I would like to highlight the importance of having enough skilled personnel in the financial entities to ensure that they are fit for DORA from day one. The FIN-FSA has recently conducted a thematic review of state of the use of new digital technologies among financial entities[1]. The thematic review also identified risks faced by financial entities in connection with the use of new technologies. The most common type of risk identified was the inadequate digitalisation expertise of personnel[2]. This was the most common risk regardless of the technology or sector of financial entity.

Evolving cyber threats and the introduction of DORA require that the financial entities have personnel with sufficient experience on ICT risk governance and management. Special expertise is also required in sourcing functions of financial entities. It is up to the financial entities´ decisions and strategic choices to ensure that these capabilities are at high level. ICT outsourcing is often heavily driven by agility, scalability and also cost savings.

Digitalisation and evolving cyber threats naturally put high demands on the management of financial entities. As DORA clearly states, the management body of the financial entity is responsible for the implementation of all arrangements related to the ICT risk management framework. This is a role that shall not be taken lightly.

[1] https://www.finanssivalvonta.fi/en/publications-and-press-releases/supervision-releases/2022/thematic-review-of-the-use-of-new-technologies-and-related-risks/

[2] This risk covers circumstances where the organisation lacks adequate expertise, or expertise is limited to a small group, as well as those where there are no experts available in the market to facilitate digitalisation.

FRANÇOIS-LOUIS MICHAUD

Executive Director - European Banking Authority (EBA)

Pave the way for DORA application

In April 2019, the EBA, EIOPA and ESMA (the 'ESAs'), sent a technical advice[1] to the European Commission, calling for a coherent approach to ICT risk in finance and recommending to strengthen the digital operational resilience of the financial services industry. In September 2020 the European Commission proposed the DORA legislation, to establish a comprehensive framework on digital operational resilience for a wide scope of regulated EU financial entities. DORA will thus provide a comprehensive rulebook and enhance the digital operational resilience of the financial sector, consolidating the various aspects of digital operational resilience, and complementing the existing prudential treatment of operational risk.

DORA mandates the ESAs to deliver a whole range of technical standards and other regulatory products by 2025, to further specify the key pillars of the legal text. This will supplement the legal framework on digital operational resilience, in particular the details of the ICT risk management framework, the ICT-incident reporting framework, the rules and scope for advanced digital operational resilience testing, the aspects of the oversight framework as well as the design of relevant templates.

DORA allows for a proportionate application of requirements to certain financial entities, particularly microenterprises, as well as financial entities subject to a simplified ICT risk management framework. Moreover, the ESAs will calibrate their rules in a proportionate manner, taking into account the financial entities' sizes and overall risk profiles, and the nature, scale and complexity of their services, activities, and operations.

DORA could further integrate ICT risk management supervision across the supervision of the financial sector via strengthening the mandates of the competent authorities and at the same time enhancing supervisory convergence across the EU. In addition, DORA will allow supervisors to obtain a complete overview on ICT-related incidents and to acquire a better understanding of ICT third-party dependencies. These will require the overall integration of DORA provisions into the current supervisory processes. It could further enhance the need for the supervisory community to keep pace with the technological developments as well as to acquire the necessary skills and talent.

DORA is a major step for addressing dependencies to CTPPs through an EU-wide oversight framework.

DORA sets the first concrete initiative to address the complex issue of the dependencies to critical ICT third-party providers (CTPPs) through an EU-wide oversight framework for CTPPs. The EBA, EIOPA and ESMA will act as Lead Overseers for the ICT risks these critical players may pose to EU regulated financial entities. They will not supervise them across the full range of their activities.

The oversight framework will build on the well-established cross-sectoral coordination mechanism of the ESAs' Joint Committee level. The Lead Overseers will conduct their oversight activities with the support of experts from the national and European relevant competent authorities. Their recommendations to the CTPPs would need to be taken into account by these competent authorities through their prudential supervision of financial entities relying on the CTPPs. Given the close cooperation and coordination envisaged for the oversight, the ESAs are already preparing for their role with a 'one team' spirit.

DORA's sectoral provisions will interplay with other relevant legislations, especially those of the Directive on measures for a high common level of cybersecurity across the Union (NIS2). DORA's oversight will complement the supervision of essential and important entities under NIS2D. This will apply to CTPPs which will be considered as essential or important entities under NIS2D.

The successful implementation of this EU-wide oversight framework will require a carefully crafted ESAs-led oversight model, along with the appropriate resources and expertise, to address coordination and consistency challenges, as individual CTPPs may serve businesses across the wider economy. The finalisation of DORA is timely and long-awaited as it contributes towards the stability and the integrity of the EU financial system.

The EBA, together with the other ESAs, are looking forward to fostering a resilient industry and will work closely together for the successful implementation of DORA.

[1] https://www.eba.europa.eu/esas-publish-joint-advice-on-information-and-communication-technology-risk-management-and-cybersecurity

JASON HARRELL

Head of External Engagements - The Depository Trust & Clearing Corporation (DTCC)

Resilient operations require a whole-of-business approach

Operational resilience has emerged as a key area of focus for supervisory authorities and financial institutions. As the financial services sector continues to experience cyber incidents impacting multiple firms, policymakers and institutions are asking: *How does my organization rapidly and safely recover from a cyber incident?*

At the same time, the financial services industry continues to undergo significant technology modernization providing new products and enhancing or expanding existing offerings. When considering this landscape, emerging technologies have provided new finance streams, expanded financial services to unserved and underserved communities, increased credit and lending opportunities for small and medium businesses, and enabled new market entrants. These advancements have also lengthened the supply chain used to deliver financial services and have contributed to the growing interconnectedness of the financial markets which could also introduce new risks.

To address growing cyber threats and their potential impacts on a significantly interconnected financial services sector, financial authorities have partnered with standards bodies, financial trade associations, and institutions to develop a framework that enhances the industry's preparedness for material operational events. As an example of the industry's resilience partnership efforts, the Digital Operational Resilience Act (DORA) represents a major step towards defining minimum controls and capabilities in the areas of cyber and ICT third-party risk management across the European Union and will help financial institutions strengthen their control in a core pillar of operational resilience. While DORA represents a significant and positive step forward, financial firms must realize that resilience is not solely an extension of business continuity or the result of strong IT and cybersecurity controls.

Business continuity and technology implementations support the delivery of resilient operations, with business areas playing a pivotal role in the delivery and sustainability of resilience across a number of functions. There are three (3) key pillars in firm's resilience frameworks where the level of business engagement is particularly important.

Financial firms must realize that resilience is not solely an extension of business continuity

Critical Operations Mapping

First, financial institutions must document and agree a consistent view of the people, processes, technology, and third parties needed to deliver critical operations. Institutions rely on different business areas to deliver products and services, with each area having its own view on how products and services are delivered based on their responsibilities. Therefore, gaining an accurate view of dependencies, across functions, will require each group to validate its role in the delivery of services. These business maps will assist organizations with understanding the true impacts of a material operational event and the potential cascading effects to other critical operations.

Tabletop Exercises

Second, no financial institution wants to experience an operationally impacting incident. However, experiencing these events without the benefit of previously exercising an organizational response only serves to increase the severity of the impact. Tabletop exercises should facilitate the business' thought process around decision-making, decreasing the operational friction that may arise when an incident occurs. Further, these exercises help the business understand where recovery is within tolerance and where additional capabilities may be required.

Capability Building

Third, the development of new capabilities is at the heart of any resilience strategy and separates resilience from risk management. Building capabilities requires business areas' support to drive integration and to validate and test solution effectiveness. By building capability, firms can close the loop and bring the business within its tolerance for disruption for certain extreme but plausible events while providing reasonable assurance for rapid and safe recovery strategies.

Resilience is more extensive than business continuity, cybersecurity, or IT solutions and more important than ever as the cyber incident and technology landscape continues to evolve. The successful delivery of resilient operations requires a whole-of-business approach to understand threat impacts to business operations, determine current capabilities to address those impacts, and gain the business insights necessary to build new capabilities and enhance existing processes.

Institutions relying solely on IT or business continuity to deliver on operational resilience may ultimately find themselves ill-equipped to execute on their resilience expectations.

It is incumbent on financial institutions to develop the governance models necessary, across their entire organization, to deliver on resilience for the benefit of the individual firm and the entire financial services sector.