BANCO DE ESPAÑA
Eurosistema

Departamento de Comunicación

27 April 2023

Digital operational resilience and business continuity

Margarita Delgado, Deputy Governor of Banco de España

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.

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

[1] Digital Operational Resilience Act

[2] Directive on measures for a high common level of cybersecurity across the Union

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.

[3] European Supervisory Agencies, namely EBA, ESMA and EIOPA