Box 2.5

THE NEW DIGITAL OPERATIONAL RESILIENCE ACT

As part of its digital finance strategy, and in order to mitigate the risks associated with digitisation and improve the resilience of the European financial system, the European Commission published in September 2020 its legislative proposal for a new digital operational resilience act, known as DORA.

After a two-year negotiation process, the final text of DORA was published in December 2023, and its date of application is January 2025.

The fact that the chosen legislative instrument is a regulation ensures that the same standard will apply in all EU countries, thus achieving an unprecedented harmonisation of ICT resilience regulation for the European financial system.

The scope of DORA is surprisingly broad, as it will apply to all types of financial institutions, of all sizes, with due proportionality. The Commission thus recognises that, given the high level of interconnections and interdependencies between the various institutions that make up the financial system, it is essential to ensure minimum levels of resilience common to all of them in order to make the whole sector resilient.

Resilience is by no means a mere compliance exercise. In a true statement of principles, the chapter on technology risk management begins with an article on governance and organisation, setting out the responsibilities and obligations of institutions' management bodies, which will need to understand these risks and be directly involved in their management. For many institutions, this will be a turning point that will force a review of the composition of their management bodies, their functions and their level of involvement in the institutions' operational resilience.

While it could be argued that DORA's requirements on technology risk management, technology incident management and reporting, system resilience testing and third-party risk management are not entirely new, it is a novelty to have elevated them to the status of a sector-wide regulation. At present, financial institutions' resilience levels are not homogeneous and, therefore, the effort they will have to make in order to comply with the DORA requirements will also differ from case to case. This is of particular concern to smaller institutions, for which it can be a major challenge to equip themselves with the necessary technical and human resources.

One of the new developments with the greatest impact on supervisors is the DORA provisions on advanced cybersecurity testing (Threat-Led Penetration Tests), similar to those already in place in some countries, including Spain, under the TIBER framework. These tests will have to be carried out with a certain frequency (in principle every three years) and will be required for a potentially large number of institutions, which will require significant supervisory resources. While some institutions already undertake these tests on a voluntary basis, for others it will imply raising standards substantially.

Also, DORA contains provisions encouraging institutions to voluntarily share threat and vulnerability intelligence, as, while the benefits of such sharing are undisputed, there is often reluctance to do so.

But, undoubtedly, the most talked-about feature of DORA, which has made the regulation a global benchmark, is the establishment of a new oversight framework for the external technology providers that are critical to the European financial system as a whole, an aspect that is becoming increasingly significant given the growing trend towards the outsourcing of certain critical functions. The Commission is aware that in order to improve the level of resilience of the sector, it is essential to take into account the technology service providers supporting institutions' critical business functions, especially those ones that have reached a systemic dimension. The new oversight scheme will be led by European supervisory agencies, although national supervisors will have to support this function.

The implementation of this oversight mechanism is requiring and will require a significant effort on the part of all the authorities in the European financial sector, including the Banco de España. Initially, procedures and methodologies will have to be developed in order to carry out effective supervision of large, complex companies with widely differing business models, organisation and governance structures, with which the financial supervisors are not familiar. Also, the authorities will have to equip themselves with the necessary additional resources, which will involve bringing in a significant number of professionals with a high level of technical expertise. This type of profile is rare and highly solicited by all types of companies, so recruiting and retaining them will be a challenge for supervisors.

Beyond the above-mentioned aspects, it is also worth noting that the regulation establishes numerous additional

obligations for the competent authorities, thereby recognising that they are key players in the ecosystem. We will need to make an unprecedented coordination effort, and play an active role beyond our responsibility as overseers of regulatory compliance, for example by promoting sectoral resilience exercises.