XIV encuentro financiero sector bancario
DIEZ AÑOS DE UNIÓN BANCARIA Y UNIÓN DEL MERCADO DE CAPITALES

Madrid, 10 October 2023

Operational resilience in EU financial services

1. Introduction:

Good afternoon, everyone, it is a pleasure to be here with you all today in Madrid on the occasion of the fourteenth meeting organised by Expansion on the finance sector. I wish to truly thank the organisers for inviting me, and for allowing me the opportunity to share my views about a growing and timely topic, namely the operational resilience in EU financial services.

As you are all aware, we are witnessing a steady pace of digital transformation across the European financial sector ranging from increasing adoption of cloud services to the broad interest in the implementation of Artificial Intelligence across the financial world. While digitalisation can provide many benefits and the participants seem to focus on leveraging those, particular attention must also be paid to new risks that result from this transformation.

This is why today I wish to touch on the importance of operational resilience across the financial sector and supporting sectors and to share relevant developments from a regulatory and supervisory perspective.

At this early stage, please allow me to clarify the term 'operational resilience', which is essential to have it clear going forward. *Operational resilience refers to the ability of a financial entity to continue to deliver critical activities for the good functioning of the financial sector during disruptions in operations*. Now, before exploring further the concept

of operational resilience and how this is linked with digitalisation, let me start by sharing some observations on digitalisation trends across the EU.

2. Digitalisation trends in financial services

The three European Supervisory Authorities (ESAs), including the European Banking Authority (EBA), are mandated to monitor market developments and to explore technological innovation and the implementation of new innovative business models. We are also looking at the innovation from the perspective of understanding the associated risks and benefits for the sector and consumers. In this context, we have been observing the strong digitalisation trend and outsourcing of services across the banking and payments sectors. Around half of EU banks (covering both corporate and retail segments) have reported that most of their customers (75%-100%) primarily use digital channels for daily banking activities. This, along with the preponderance of digital payments, is one clear indication of the growing adoption of digitalisation in consumers' daily finance activities.

In the area of Artificial Intelligence (AI), more than 70% of EU banks use AI at least in some areas of activities. Its use is more widespread in creditworthiness assessment and credit scoring, fraud detection, commercial profiling and clustering of clients or transactions, AML/CFT being more wide-spread. An increased use of chatbots or similar solutions is being noticed. We also see that many financial entities focus on optimisation of internal processes and introducing digitalisation in order to increase efficiencies and cut their operating costs.

On the risks side, growing operational risk has been noted with cyber risk and data security reported as the main sources where other sources of operational risk are also becoming relevant such as IT failures.

Collaborations have also been developed in commercial and distribution activities. Probably, you may be well aware that this transformation comes with strong reliance on technology providers which provide ICT services to the EU financial entities. Indicatively, 65% of EU banks reported they have established partnerships with BigTech firms, mainly to facilitate distribution of financial services and non-financial services. Such partnerships, which are increasingly gaining importance in the banking sector, could create additional complexity of existing infrastructures, where such providers could leverage their network effects and data collection superiority. The wider use of partnerships and increases the dependence on ICT providers, which is also observed in the area of regulatory compliance where the use of technology has increased quickly. It is becoming evident that digitalisation is deepening interconnections and dependencies within the EU financial sector and with third-party infrastructure and ICT providers. I would like to focus a bit more on this and in particular the dependency on ICT providers and their role in strengthening operational resilience across the EU financial sector.

3. More digital but also more reliance on ICT third-party providers

The growing reliance on ICT providers can potentially create risks to financial stability. Such risks can be magnified if the reliance is on a single or small number of ICT providers, especially in situations where the services offered by them cannot be easily substituted by the financial entities or other providers, considering the impact on the EU financial sector in case these providers or their services are disrupted or fail.

From the financial entities' perspective, dependency on ICT providers and inability to easily replace the services offered by them is an operational challenge mainly to determine how they can maintain critical functions operating in a resilient manner. These guarantees must also be explicitly included in the contractual clauses that govern existing contracts. From supervisors' perspective, there is a challenge of how to gain assurance of financial entities' risk management and operational resilience and whether ICT providers are introducing additional risks that could impact the financial sector.

As a result, the supervisory and regulatory framework both at international and EU level is progressively adapted to further focus on operational resilience. The concept of operational resilience builds on the prudential operational risk framework, encompassing the mechanisms of internal governance, the rules of outsourcing, business continuity and relevant risk management-related aspects. The ability to deliver on the contract conditions during disruptions can help a financial entity to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations during disruptions.

At international level, we already have a set of principles for operational resilience for the banking sector, for example, those set by the Basel Committee on Banking Supervision (BCBS) in March 2021) while a review of the Financial Stability Board's principles that should apply to third-party providers is underway. These aim to strengthen financial entities' ability to withstand operational risk-related events that could cause significant operational failures or wide-scale disruptions in financial markets.

At EU level, a new legislation on digital operational resilience for the financial sector (DORA) has entered into force in January 2023 and it will become applicable to almost all EU financial entities from January 2025. DORA was inspired by the international standards in the area and its purpose is to put in place a comprehensive framework on digital operational resilience across the EU financial sector. The first pillar of DORA aims at consolidating and upgrading ICT risk requirements that have so far been spread over in different texts of the financial services legislation and to foster convergence and efficiency in supervisory approaches when addressing ICT risks (including ICT third-party risk) in the financial sector. It essentially aims to highlight the importance of ICT risk by distilling it from the financial risks, noting the need for a comprehensive assessment of these risks.

The second pillar of DORA introduces an EU-wide oversight framework for the ICT providers that are assessed as critical for the EU financial sector. The aim is to ensure that EU financial

entities relying on such critical providers are not exposed to critical ICT risks that may compromise financial stability across the EU economy. I will come back to the upcoming DORA oversight framework in a bit.

4. Current ICT TPPs' landscape in the EU financial sector

The new regulation, DORA has given new roles and tasks to the three European Supervisory Authorities hence we are currently developing the complementary level 2 regulatory texts that allow the application of this Regulation and the design of the new supervisory framework. In relation to this work, we have conducted a high-level exercise to trace the landscape of ICT providers in the EU financial sector. The objective was to obtain a preliminary overview of the provision of ICT services to the EU financial entities by ICT providers.

The exercise was carried out based on information provided on a best-effort basis by a sample of EU financial entities (representing different segments of the financial sector) focusing on the services they receive from ICT providers. Overall, the exercise has identified around 15,000 ICT providers directly serving EU financial entities. The providers offer a large range of ICT services and most financial entities. The most common ICT services were (i) software and application services, (ii) ICT consultancy & direct management of processes and (iii) cloud computing services. The type of ICT services that mainly support the critical and important functions of the EU financial sector are (i) network infrastructure services and (ii) data centre services.

The results of our joint analysis also reveal a highly concentrated market despite the high number of ICT TPPs identified and the number of ICT services provided. Frequently, the suppliers that provide services for the operation of most critical functions are not replaceable or the contingency of alternative suppliers is not foreseen by the financial institution., which exacerbates the concerns over the concentration risk in the sector. In addition, a potentially high degree of interconnectedness and interdependencies between ICT providers were observed in the exercise.

I would like to take the chance to thank all the industry participants who have voluntarily contributed to this exercise as its results have provided very valuable data to the process of developing the regulatory framework and the preparatory work of the ESAs on the new supervisory framework (for example, in determining what the criteria should be to determine a supplier as critical/essential).

5. The ESAs' upcoming role in overseeing critical ICT third-party providers

Allow me to go back to the supervision model foreseen in DORA and outline briefly how the new legislation aims to address potential systemic and concentration risks posed by the EU financial sector's reliance on a small number of ICT providers. In terms of type of

ICT providers, DORA covers a wide range, including providers of cloud computing services, software, data analytics services and providers of data centre services.

You may wonder how this new oversight will work. As a first step, the ESAs will collect data from the EU financial entities (via their competent authorities) on the ICT services they receive from ICT providers and on those providers. Based on these, the ESAs will designate the *critical* ICT providers for the EU financial sector taking into account a number of criticality criteria. This exercise will be done on an annual basis and the list of critical ICT providers will be published. Each critical ICT provider will be overseen by one of the ESAs (Lead Overseer) where essentially the ESAs will be assessing whether each provider has in place adequate mechanisms to manage the ICT risks to which they may expose EU financial entities. Recommendations and lines of improvement will be issued to address the weaknesses detected. If these reports are not made or are not considered sufficient, action may also be taken via the supervised financial entities that receive services from that provider, requesting reports on the way in which the service is provided, or ultimately the identification of alternative providers.

This is an innovative framework.

To make this work, it would be essential to ensure proper collaboration between the ESAs and EU financial supervisors. Therefore, the ESAs will be setting out a comprehensive cooperation and coordination framework building on the existing institutional architecture enhanced by new structures.

- First, the existing Joint Committee of the ESAs that already facilitates cross-sectoral coordination, including on ICT risk, will be supported by a new Oversight Forum. The latter will have steering and consultative powers and will bring together representatives of all relevant competent authorities, with the aim of promoting a consistent approach to monitoring ICT third party risk and designating critical ICT providers at EU level.
- Second, a Joint Oversight Network will be responsible for the coordination of oversight activities among the ESAs.
- Third, at operational level, Joint Examination Teams will be established for each critical ICT provider which will be composed of the ESAs' and competent authorities' staff to carry out the oversight activities.

Due to the inherent cross-border nature of the provision of certain ICT services, the Lead Overseer may also exercise its powers on premises in a country outside of the EU which is used by the critical ICT provider to provide services in the EU – a very important element of DORA considering the landscape of ICT providers. For this purpose, DORA envisages the possibility for the ESAs to conclude cooperation arrangements with third-country authorities.

6. Conclusion

To conclude, I firmly believe we all need to work together to make the EU financial sector more resilient as
as we move forward in implementing technological improvements in the efficiency of the sector. The objective is to ensure technological safety and good functioning as well as quick recovery from ICT breaches and incidents to enable the effective and smooth provision of financial services across the EU, including under situations of stress.

It is crucial for financial entities to leverage all improvement mechanisms of operational risk management to achieve operational resilience and to recognise its importance alongside financial resilience. Furthermore, we all need to acknowledge that operational resilience is more than just business continuity, a concept familiar to the sector for many years. The identification and individual management of all critical functions in conjunction with the end-to-end view, the focus on the evaluation that any disturbance may have the use of the tolerance and risk appetite as criteria for disruption to drive decisions about resilience investment, and the consideration of providers' own resilience with which an entity works.

The overall objective, namely to strengthen and align the operational resilience across the EU financial sector is challenging, and to achieve this DORA is a welcoming development, to which the EBA, together with the other ESAs, is looking forward.