Jose Manuel Campa's Keynote speech at Annual Assembly of the Spanish Banking Association

Madrid, Spain -0 11 April 2024

Cyber resilience and financial innovation, getting ready for the new challenges

Introduction

Thank you for inviting me, it is my pleasure to speak here at the Annual Assembly of the Spanish Banking Association.

Financial institutions have been increasingly relying on innovative technologies to provide their services in a digitalised world. Innovation is an inherent force of the evolution in economic history: the Austrian economist Joseph Schumpeter coined the term of "creative destruction" to indicate how traditional businesses and economic models are replaced by the appearance of new technologies, or new applications of existing technologies, which in turn have the power to change how products and services are delivered. However, compared to past waves of innovations, and looking, in particular, at the financial sector, the key novelty of the digital transformation we have been experiencing over the last decade is its pervasiveness, leading to new interconnections and interdependencies.

These interconnections often occur between incumbent financial institutions, FinTechs and BigTechs through a variety of models, like partnerships, joint ventures, outsourcing and sub-outsourcing. Digital platforms are increasingly used to market and distribute financial products and services, sometimes bundling different financial and non-financial services and products from a range of providers. This has contributed to a substantial re-design of value-added chains: new

players may emerge that are active in the financial sector both through the provision of services to financial institutions – often for critical functions - but also through direct provision of financial services such as lending and payments.

These evolutions have brought benefits for those financial entities that were ready to grasp the potential of innovative technologies and could then find themselves in a better competitive position. In addition, many of the innovations led to an improvement of the consumer experience, e.g. allowing access to financial services on a 24/7 basis, reducing transaction processing times and costs and providing cross-border services more efficiently.

It is of course the task of prudential regulation to properly assess the impact of those changes and set the boundaries to ensure that their introduction result in an enhanced provision of services and risks are properly managed.

Risks from digitalisation of financial services

For all these opportunities to be leveraged responsibly, it is now clear that the industry, supervisors and regulators must be able to identify, monitor and mitigate risks that are often inter-related. Today, I would like to focus on three areas: the increased threats of cyber incidents and cyber-attacks, including in a context of increased geopolitical tensions, the high level of operational interconnectedness between financial entities and ICT third-party providers (including the high level of concentration risk), and the introduction by financial entities of new technologies and new cooperative arrangements in the provision of their services.

Cyber incidents are likely to result in service disruption and these disruptions are also more likely to become more severe, due to increase complexity and interconnections. In addition, cyber-attacks in the financial industry is an increasing area of focus. Several data support this picture. In its Foresight 2030 Threats report issued in September 2023 , ENISA identified “Supply chain compromise of software dependencies” as a relevant threat: increased integration with components and services from third parties could lead to disruption, malfunction, data loss and leakage. In their 2022 Annual Report , the FSB indicated how frequency and sophistication of cyber incidents are growing rapidly and have spill-over effects across borders and sectors. Furthermore, we are all well aware that during the past two years, the cyber threat landscape has further evolved due to the rise of geopolitical tensions. Digital financial crime is also playing an increasing role, leading to further threats to information security and business continuity.

In the EBA Risk Assessment Report issued at the end of last year we show that cyber risk and data security continue to be by far the major drivers of operational risk for banks, with one third of respondents also pointing to ICT failures as an important factor. EU banks moreover reported a rising number of new ICT risk events, about 61,000 IT risk events reported in 2022 an increase of over 20% from 2021. The Risk Assessment Report shows that – despite continuous investments in ICT security infrastructures - the share of banks having been victim of up to ten successful cyber-attacks increased rapidly since the first half of 2022.

On the positive side, and this is quite encouraging, a large majority of responding banks reported that they actually did not face a successful attack which resulted in an actual major ICT-related incident, which may indicate overall progress in managing ICT risks.

However, this encouraging evidence so far should not lead us to complacency. On the contrary, as the reliance on these technologies and the complexity of the interconnections increase so must also increase the focus of institutions in insuring overall resilience. Which brings me to my second theme.

DORA: the regulatory response to increased cyber resilience risks

This increasing relevance of risks stemming from the pervasive use of ICT tools led European legislators to introduce the Digital Operational Resilience Act (DORA), which became into force in January 2023. With DORA, for the first time, a comprehensive framework on digital operational resilience across the financial sector is being established, thus consolidating and strengthening those ICT risk management requirements that until now were spread over financial services legislation.

DORA harmonised the rules in major areas such as ICT risk management; ICT incident management and reporting; testing of the digital operational resilience of ICT systems; and the management of ICT third party risks. On top of that, for the first time at EU level, DORA establishes a new framework for the oversight of critical ICT third-party service providers (CTPPs).

With DORA, the EBA and its sister ESA authorities, EIOPA and ESMA have been given a central role, in two respects: (i) the development of several of policy mandates complementing DORA; and (ii) the establishment of an oversight framework over CTPPs, for which they will also be responsible. We have started working on these two areas in 2023 and will continue through this year, to ensure DORA is fully applicable in January 2025.

On the policy area, we have developed a set of draft technical standards on which we have consulted on a first batch in summer last year and on a second batch in the first months of this year.

Let me acknowledge that in all cases the public consultation showed an exceptional level of engagement by a wide variety of stakeholders, both in the participation to the public hearing and to the number of responses received, which reached 100-120 for certain products. While this clearly shows the interest of the industry for DORA and its application, it also allowed the ESAs to refine and adjust the products before submission to the EU Commission.

First, stakeholders flagged the need for more proportionality and clarity aspects, and we tried to reflect this in the RTS on ICT risk management. Similarly, smaller and non-complex entities have been exempted from the application of some requirements and many proposed classification thresholds have been increased.

A second concern was related to the overall complexity and prescriptiveness of the mandates. The final RTS on risk management framework integrates a risk-based approach to the extent possible and the classification approach and criteria for major incidents have been simplified and streamlined to limit the burden to financial entities, focusing more on the impact of the incident.

We also addressed a third concern from the industry, i.e. consistency of the requirements across different sectors, considering that some operational resilience and ICT risk management requirements have already been put in place. This is a critical aspect, given the scope of application of DORA, which includes financial entities of different dimension, sectors and level of ICT maturity.

While the implementation of these new requirements might pose challenges for some financial entities, others are already subject to sectoral ICT risk management requirements, which bring them closer to DORA expectations. However, the feedback from public consultation hinted at some areas where room for a more general improvement still exist, for instance on subcontracting management. Therefore, there is benefit for the financial sector to use the time until the application of DORA, and to upgrade their ICT risk management to bring it in line with the new framework.

A new role for the ESAs: the oversight framework

The second task that EU legislators assigned to the ESAs through DORA is the responsibility for the oversight of critical third-party providers starting in January 2025. From an operational perspective, we are working as one single team to ensure that the oversight operating model will function properly. There are two aspects which deserve particular attention: first, the identification of the third-party providers to be designated as critical, second the cooperative feature of the oversight framework.

The process of CTPP identification and designation relies on the completeness of information and on the quality of data. In this regard, a key role is played by the Register of Information on the contractual arrangements on the use of ICT services provided by ICT third-party service providers, which financial entities shall make available to their competent authorities.

Secondly, is the homogenous application of the oversight across all the financial sector. Continuous cooperation between national authorities and the ESAs will be essential to ensure a smooth functioning of the oversight framework and avoid overlaps and duplication of requests to third party providers.

Cyber-risks increase the need for fast communication and more efficient supervisory coordination

I cannot end my considerations on cyber-resilience without reminding of the importance of information exchange and action coordination at a time when the news of a cyber-threat has the potential of spreading around the financial sector in a few hours, with relevant consequences on the stability of financial system.

Under DORA, the ESAs will play a key role in coordinating information sharing on major ICT-related incidents and significant cyber threats between competent authorities and we will establish mechanisms to enable the sharing of effective practices to enhance situational awareness and identify common cyber vulnerabilities and risks across-sectors.

Exchanging information between financial entities is also an important element for ICT risk management framework to be effective, as it could facilitate the prevention and the early detection of ICT-related incidents. This is why DORA encourages financial entities to exchange information on cyber threats.

Digitalisation trends

Technological innovations are affecting financial services and financial stability in a much broader sense than operational risks from the introduction of ICT technologies. So, let me also provide a brief overview of our wider work on innovative applications in the financial sector, which requires a continuous focus.

Let me quickly highlight three broad topics that will be our focus in 2024/early 2025: (i) tokenisation, crypto and DeFi, (ii) AI/ML, and (iii) value chain evolutions.

Tokenisation, Crypto and DeFi

Turning to the first of these areas, banks are increasingly leveraging distributed ledger technologies in their business processes and are exploring the possibility to issue tokenised deposits as a settlement instrument.

Indeed, data from our autumn RAQ exercise, identifies that 62% of respondent banks are exploring, developing, experimenting with or using DLT, and around 50% of respondent banks are specifically exploring tokenisation of traditional financial assets, including deposit tokenisation.

In view of these trends, the EBA is taking forward further work to assess the opportunities and risks and identify any areas in which supervisory convergence or regulatory efforts are needed.

One example is our ongoing stocktake of potential models for deposit tokenisation, to inform supervisory dialogue with a view to promoting a common understanding of opportunities and risks and developing a common supervisory stance.

More broadly, on crypto-assets and decentralised finance, in addition to the EBA's policy and supervision and convergence work under MiCAR, the EBA will be reporting to the European Commission later this year on some activities that fall outside the scope of MiCAR.

Crypto lending and staking activities fall outside the scope of MiCAR and have increased in recent years, albeit from a low base . Some risks of consumer detriment have been observed, for instance as regards poor (if any) disclosures of terms and conditions, complex business models, conflicts of interest, and lack of clarity regarding enforceability of claims.

Artificial intelligence/machine learning

The use of AI/ML applications continues to grow with a substantial majority of EU banks using these applications in a range of business processes such as customer profiling, fraud, money laundering and terrorist financing detection, and creditworthiness assessments.

The new AI Act, which is a 'horizontal' policy initiative will apply to the EU banking sector – and questions are emerging from both industry and the supervisory community about how the new requirements will intersect with existing sectoral measures.

In light of these questions, in 2024 the EBA will take stock of the new AI Act and perform a comprehensive mapping of existing and upcoming prudential and consumer protection requirements on the use of AI in the banking sector, primarily focusing on creditworthiness assessment of natural persons. The objective is to provide an assessment of the areas where additional guidance, clarity or harmonisation may be needed regarding supervisory expectations on the use of AI. I would expect us to report on the outcome in early 2025.

In the meantime, we will continue to monitor market developments, including potential uses of generative AI in the banking sector, for instance via industry and supervisory dialogue.

Value chain evolution

Turning now to technology-facilitated value chain evolutions, we know the industry is transforming the way services are compiled and market to their customers . As usual, these changes bring opportunities and risks. This year we will be focusing on the growing phenomenon of the distribution of banking products via 'white labelling' to explore business models, and any specific risks, for instance in terms of consumer protection, money laundering, and supervisory visibility.

Beyond these areas of thematic focus, the EBA will continue its wider contributions to ongoing legislative and other initiatives, for instance in the context of the digital euro and open finance, and our ongoing efforts to facilitate dialogue between industry and supervisors on RegTech and SupTech developments, not only to foster the development of complementary technologies, but to 'deep-dive' into specific cases that could support EBA and competent authorities in performing the new oversight and supervision tasks under MiCAR and DORA.

This is important work to ensure that, as a supervisory community, we too reap the benefits of innovation in the performance of these tasks, and in other areas, such as the sustainable finance initiatives.

I thank you for your attention and, of course, am happy to respond to questions.