Cybersecurity and digital operational resilience

1. DORA implementation progress

1.1 Overall progress made with the implementation of DORA and next steps

The Chair explained that the Digital Operational Resilience Act (DORA) aims to enhance digital operational resilience in the financial sector. It takes an ecosystem approach extending to ICT third party providers and covers a number of interlocking facets, such as risk management by financial entities, third party risk management and outsourcing, incident reporting, threat led penetration testing and the new oversight framework for critical third party providers (CTPPs). The Level 2 regulatory technical standards (RTS) are being completed. The first set of RTS was adopted by the Commission earlier in the year, and the second set is due to be adopted in the near future. Proportionality is embedded throughout the regulation. The main focus is now on implementation, given the planned start date of 17 January 2025.

A regulator stressed the need for industry players to begin preparing for the implementation of the DORA RTS, even though they are not yet fully adopted, as significant changes to them are unlikely. The first priority is to establish the information registers mandated under DORA, which are designed to ensure transparency, accountability, and facilitate oversight in the management of ICT risks within the financial sector. Once these registers are in place, they will allow for better mapping of potential contagion channels and provide a clearer understanding of how incidents involving different levels of third-party providers might impact financial entities. The second key priority for financial institutions is reviewing their contracts with ICT providers against DORA requirements. This requires developing a comprehensive plan to establish new, balanced relationships with their third-party providers. This will be a significant effort, as many existing relationships with third parties have been in place for years.

A dry run exercise was conducted during the summer to help financial institutions and regulators evaluate their readiness to implement DORA. On a voluntary and best efforts basis, 1,000 financial entities from 20 member states took part in the exercise, supported by the national competent authorities (NCAs). The preliminary results show that only 2% of entities achieved fully adequate results. Around 50% did not demonstrate an appropriate level of readiness. It is clear that further work is needed to prepare the implementation of DORA. The feedback documents of this exercise will set out the best practices and areas of improvement that were identified, together with further guidance for market participants.

An official noted that the UK has also made good progress on tackling cyber and digital operational risks, which are considered as one of the top risks facing financial firms. The UK's operational resilience, outsourcing and third party risk management policies are due to be implemented by March 2025. Critical third party (CTP) oversight is another regulatory priority that is being addressed. These frameworks will address a broad range of risks, including new developments such as artificial intelligence (AI) and quantum computing.

1.2 Preparation of the implementation of the CTPP oversight framework

A regulator explained that the new CTPP oversight framework is an important and innovative part of DORA. A common structure will be created by the three European Supervisory Authorities (ESAs) to conduct the oversight of CTPPs and ensure their operational resilience in a consistent way across the different financial sectors. Each CTPP will have a lead supervisor, but the aim is to create consistency in the regulatory interactions with CTPPs, using the same oversight methodologies, risk assessments and tools and reporting systems. In addition, resources with adequate IT skills must be available to conduct the oversight. The ESAs have been recruiting additional staff, but two thirds of the resources will come from the NCAs.

An industry speaker explained that their firm, anticipating designation as a Critical Third-Party Provider (CTPP), established a cross-functional working group in 2022 to proactively prepare for DORA compliance and to assist customers in navigating the upcoming requirements. Cybersecurity and operational resilience are long-standing areas of focus, but it had to be ensured that internal processes for testing and resilience meet the requirements of DORA and that these requirements are embedded in internal controls and governance. Contractual agreements with customers also have to be reassessed. The structured two way dialogue that is due to be implemented between the authorities and the industry should help improve risk management and resilience further across the financial sector. In addition to the DORA implementation, there is also an ongoing discussion on the EU's voluntary cybersecurity certification scheme. ENISA's recent updates are welcome, particularly the introduction of a three-tier certification system and the removal of some sovereignty-related requirements. These changes are expected to encourage broader adoption of the scheme across Europe.

An official stated that the Bank of England, the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) are developing a UK regime for critical third parties (CTPs), which will be similar but not identical to DORA. Due to the timing of the recent UK election, the regime will be finalised later in 2024. During the consultation process, the industry supported the objective of enhancing the resilience of the financial sector and

provided positive feedback on the proposed regime, but there were also comments on the challenging granularity of the regime.

1.3 Expected changes with DORA

An industry representative considered that DORA is a significant step forward in managing ICT risks, although it is not certain that it would prevent complex failures such as the CrowdStrike global outage in 2024, which disrupted interconnected systems worldwide. There is a need for preventative actions and a proactive approach, such as the enhanced testing and reporting obligations and CTPP oversight introduced by DORA.

The true effectiveness of DORA will however depend on its real-world application and enforcement. The impact of improved testing and reporting systems will need to be monitored over time, with a focus on how reporting can provide data that can help stop attacks, especially since current testing is performed at set intervals rather than in real time. Additionally, proportionality is key: while DORA's impact on financial institutions of different sizes is often discussed, its effects on technology companies of varying sizes must also be considered. It is hoped that the issues that smaller tech companies experienced with GDPR will not be repeated now we have the hindsight of that experience. This aspect requires further attention within DORA's framework.

A regulator commented that a situation as complex as CrowdStrike might be difficult to avoid completely, but the registers of information in DORA will help alleviate contagion risk.

A second industry speaker emphasised that the focus on testing, reporting and preventative measures is essential in light of the changing nature of cyberattacks and the increasing reliance on third parties. DORA does not introduce anything fundamentally new, but it will create a significant shift across the whole industry. Financial institutions will have to undertake more systematic third party risk management, involving more regular and real time reporting, monitoring and testing.

2. Challenges raised by the implementation of DORA

The Chair highlighted a number of challenges to overcome in the implementation of DORA. The first challenge is DORA's ecosystem approach. There will need to be rigour to get the whole ecosystem moving and ensure there is real improvement across the industry. Second, the supervisory community will need to maintain momentum to ensure that DORA is implemented in a timely manner. Firms in the ecosystem are currently at different levels of maturity in terms of cyber resilience, but they all need to move forward together to achieve a consistent level of high-quality implementation. Finally, addressing resource scarcity is a key priority in the implementation of DORA.

An industry speaker agreed that making a significant change to the entire ecosystem, which includes a great variety of players of different sizes, is challenging. Some market participants do not have sufficient resources to make the required changes. Secondly, the adoption of new technology and change processes necessary to implement DORA will be a step change for many institutions. It will require additional resources, technical expertise and the buy in from senior management. Although all players need to progress, the nature and timescale of the evolution required might vary according to the size of the player.

A regulator considered that the main challenges to be addressed by supervisors in the implementation of DORA relate to the CTPP supervisory regime. The first challenge is capacity building. At NCAs, resources with supervisory experience will need to be redeployed and trained to conduct CTPP oversight. Secondly, the ESAs and NCAs must coordinate their actions to avoid duplication or contradiction, including with other authorities such as the ECB and ENISA. Finally, there must be greater mutual learning between authorities and third party providers to ensure that CTPPs understand what is expected from them and that authorities can implement oversight appropriately within the planned timeframe of 2025. Further policy developments are not needed in this area for the time being. The priority is to implement DORA and the other digital regulations that have been adopted. Some refinement of DORA's interactions with the existing regulations on ICT risk and operational resilience might be needed however, such as eliminating any duplication.

An official highlighted that establishing a common understanding of how the oversight regime for CTPPs will function is essential. That will represent a significant change in terms of culture, because the institutions concerned are unaccustomed to being regulated by financial services authorities.

A second industry representative noted that the implementation of DORA will require financial entities to review the existing contracts that they have with IT third party providers. Some financial institutions do not feel like they have enough power to renegotiate the right service level agreements (SLAs) with large tech companies. In this regard, proportionality is also important.

A third industry speaker agreed that the scarcity of resources with cybersecurity skills is a key challenge. A further aspect to be considered, as stated in the Draghi report, is that Europe needs to find a middle way between promoting its domestic cloud industry and ensuring that European financial entities can access the right technology to ensure the security and resilience of the EU financial sector.

3. Tackling system wide cyber risks

An official emphasised that the systemic dimension of cyber-risks must be considered, beyond the operational resilience of individual firms. As the financial sector is one of the most protected, significant cyber-risks have not yet materialised, but disruptions to other vital activities, such as hospitals, caused by cyber-attacks show the importance of preventing these risks. Concentration risk is particularly challenging in the financial sector because financial institutions often

operate homogeneously to reduce costs and use similar tools. Regulators also seek a common framework for efficiency reasons. But this uniformity increases vulnerability to cyber-attacks. Introducing some controlled inefficiencies or duplication could actually help mitigate cyber risks. The Chair remarked that the establishment of registers of information under DORA will facilitate the identification and tackling of concentration nodes.

The official also identified three changes that need to be considered by regulators in the fight against systemic cyber risks. The first is a cultural change, as traditional prudential regulation is not sufficient to address these risks, and new approaches are needed that take into account technology choices and data protection. Second, these risks need to be addressed on a system-wide basis from the outset, rather than focusing initially on individual financial institutions. Finally, the credible risk that central banks could also be targeted by cyber-attacks needs to be taken into account in the development of cyber resilience strategies.

The pan-European Systemic Cyber Incident Coordination Framework (EU-SCICF) was developed in collaboration with the Bank of England and the ESAs to mitigate the risk of a coordination failure during cyber incidents. This mechanism aims to improve the preparedness of authorities and ensure a consistent response to major cyber threats by facilitating the collection and sharing of information between authorities, allowing for better assessment and coordinated responses. The EU-SCICF is well integrated into DORA through Article 49, which establishes a coordination mechanism between supervisory authorities.

Another official stated that the priority for the UK, which is consistent with the objectives of the EU-SCICF, is to ensure that effective arrangements are in place to handle crisis situations. This means that all stakeholders need to be aware of their roles and effectively coordinated during an operational resilience incident. Cooperation during cross border incidents is critical to remediating them properly. In general, supervisors are used to thinking about risk from a micro prudential perspective and making sure that individual firms are operationally and financially resilient. With digital operational resilience comes the need to think about risk at a system wide and macro prudential level, however, which requires a better understanding of data and the interlinkages within the system. There is work underway on this subject at the Bank of England and the European Systemic Risk Board (ESRB), but this is a significant change in the mindset of the supervisory authorities. Further exploratory work is required before deciding on the policy tools, which could include the creation of additional redundancy in the system.

An industry representative stated that one key question with regard to financial stability is whether some tech companies have become 'too big to fail', for example if they operate a piece of infrastructure that poses a systemic risk. CrowdStrike is an example of the impact that a tech provider can have in the financial market and beyond. The testing performed before the roll out of the technology was clearly insufficient, but there is still a lack of clarity on whether it is the responsibility of financial institutions to ensure that tech companies have properly tested their technologies or whether the relevant regulator should ensure that the tech company has performed adequate testing before deploying its software.

4. Further issues to consider

4.1 Cooperation at the EU and international levels

An official explained that operational resilience issues are cross border by nature and financial entities are exposed to cyber risk originating in other jurisdictions, which emphasises the need for coordination between authorities at international level. All authorities need to work together to fight cyber risk, and this approach already exists for other forms of prudential regulation. The UK authorities have bilateral arrangements with a number of authorities, participate in global colleges and also engage with international standard setting bodies and groups like the G7 Cyber Expert Group. The Chair agreed that these ecosystems are not restricted by national boundaries. While much work has been done by the FSB and other international organisations, there is much more to do on cross border cooperation.

An industry speaker highlighted the need for harmonisation and a shared vision across all authorities in the EU. It is positive that the three ESAs have formed a common structure for implementing DORA, but all European financial supervisors need to have the same understanding of the texts to ensure that the detailed guidance does not create confusion or contradict the Level 1 regulation. The 27 national transpositions of the Network and Information Security Directive (NIS2) also need to be aligned with DORA, and DORA itself needs to be aligned with other global third party frameworks, such as the UK's CTP regime. There might be a steep learning curve in the short term, but consistency should be attainable over time.

Another industry representative emphasised the importance of knowledge transfer, especially from technology companies to regulators and the IT departments of financial firms. This needs to be done properly to ensure the right skills are in place. There needs to be a more collaborative approach than is typically seen in regulation and a more transparent approach with more information sharing. These culture shifts will be a prerequisite for success.

4.2 Supply chain risks

The Chair noted that one of the aspects being discussed as the draft regulations are being finalised is how to capture the interface between financial firms and their wider supply chains and how to strike the right balance of responsibilities along the supply chain in a pragmatic and proportionate way.

An industry speaker remarked that the evolving nature of supply chains has increased the scope for attacks and is a key driver of cyber risk. This can be mitigated by using real time monitoring tools and ensuring that all players along the value chain use common frameworks in a

consistent way. In this regard, it is essential to be proactive and use predictive threat analysis. With increasing interconnection, cyber risk propagates along the value chain both downstream and upstream. Continuous monitoring and reporting is needed to fight these evolving cyber risks.

4.3 The role of AI

An industry representative stated that the huge amount of data that has to be collected and analysed to fight cyber risk requires the power of AI. Cyber-attackers are already leveraging AI technology to identify vulnerable targets in the financial services sector and design attacks. The financial ecosystem needs to use the same tools. AI is a tool that can help stress test and model different response scenarios for the whole ecosystem, which is much more complex than for an individual entity.

Another industry speaker agreed that the impact of AI needs to be assessed in terms of how it is changing the threat landscape and how it can support cyber-security teams. While AI will not replace security teams, it will help to bridge the resource gap and support their actions.