Cyber and digital operational resilience

1. DORA implementation: progress and next steps

1.1 Overall progress

The Chair stated that the post Level 1 negotiations on the Digital Operational Resilience Act (DORA) implementation began 12 months ago. On 19 June 2023, the first of the two main consultations on the implementation of DORA was launched by the European Supervisory Authorities (ESAs). This consultation covered four topics: the risk management framework that DORA seeks to establish; the classification of major incidents for reporting purposes; the register of outsourcing arrangements; and the policy requirements for outsourcing to third parties.

Four key principles are guiding the implementation of DORA: momentum, pragmatism, quality and proportionality. Momentum is important due to the tight timelines that have been agreed and the material risks involved. It is vital to be pragmatic because this is a highly complex area with only a short period of time in which to achieve implementation. This means reaching a compromise on the Level 2 requirements with a level of detail that is not excessive. There is also a commitment to a high quality standard in the ongoing work and proportionality has been integral to the proposals.

1.2 Ongoing consultations

Asked to comment on the key aspects of the DORA implementation and the related ESAs' consultation documents, a regulator explained that the consultation process plays a key role in the formulation of the final framework and also allows regulators to engage with the industry and test and share ideas. It is still work in progress. The consultation on the first batch of documents concluded on 11 September. Four sets of provisional documents were published on information and communication technology (ICT) risk management and incident reporting. The aim is to finalise these documents, taking into account the feedback from the industry and other stakeholders, and make proposals on the approach to the implementation of the requirements by the end of 2023. There are many complex and multifaceted issues to address however, for which further specification will be needed.

It will be important not to place an excessive operational burden on ICT providers and financial entities and for this, proportionality is extremely important. There is still conceptual work to do on the classification of incidents and the categorisation of services. It will also be important to define the scope of the requirements, in particular whether they will apply to registers of information, the level of application at group and solo level, the required level of consistency, how engagement with firms will be conducted and the level of flexibility granted to providers and financial entities. These elements must be calibrated and fine tuned before the end of the consultation. At the same time, the ESAs are also working on the incident reporting framework and developing a proposal for advanced testing.

The regulator added that the ESAs are preparing a second batch of policy documents. A response will soon be published to the Call for Advice (CfA) issued by the Commission on the criticality assessment and the oversight fee model. The methodology will be contained in a second instalment, which will be published within six months of the Commission's adoption of the delegated act, which is likely to be at the end of 2024.

2. The main challenges raised by the implementation of DORA

The Chair stated that the implementation of DORA is unusually complex and will require a huge amount of preparation and interaction between regulators and the financial industry. It is cross sectoral; it affects all firms, large, medium and small; its reach is global, European and national. The outsourcing registers are a good example of the complexity involved. A financial group might have numerous points of entry, and a third party provider (TPP) might have numerous relationships in terms of sub outsourcing arrangements.

2.1 Challenges for market participants

A Central Bank official suggested that there are three main challenges for market participants. First, while some financial institutions were already included in the European Banking Authority (EBA) outsourcing guidelines, which provide a sound baseline for implementing DORA, the firms outside the scope of those guidelines are now facing a true shift in expectations, which will require significant efforts. Secondly, all market participants will need to update their existing contractual arrangements with CTPPs to include a number of mandatory provisions. Finally, market participants working with the CTPPs included in the scope of the oversight framework will likely face higher expectations from supervisors.

An industry representative explained that many financial institutions are in the gap analysis phase. They have assessed the potential impacts of DORA and they are starting to make plans and budgets for implementation.

Firms are facing both common and specific challenges. The first common challenge is around capacity and resources. There is significant demand on teams managing resilience and cybersecurity and a shortage

of talent in this space. For global firms, there are also problems of global consistency, with other jurisdictions, such as Australia and the US, also seeking to implement their own frameworks in this area. The second common challenge relates to the business case and strategic aspects of DORA. As teams seek to implement DORA, they are seeing DORA both as a compliance exercise and a way to create competitive advantage. In advance of implementation, some firms are trying to better understand the intent behind the requirements in order to drive more effectively the cultural change required to embed DORA in their organisation and make the changes sustainable.

Some firms face more specific challenges. First, the focus within DORA on data classification has significant consequences for issues such as access management, data backup and encryption. These are notoriously difficult topics, notably for legacy systems and only few firms really grasp them well. Secondly, DORA will be a significant step change for some firms, particularly the smaller ones and those that do not have sufficient technical capabilities or experience in this field. Organisational changes or changes to operating models might also be needed. Some of the more challenging aspects of DORA are the ability to restore data from backups to new systems in order to address ransomware threats; the need for a control function to oversee and manage ICT risk; and the focus on threat led penetration testing. The final challenge is around the scale and complexity of the TPP ecosystem. The topic of fourth party providers is hugely challenging, for example, due to the issues around exit strategies and the substitution of third parties. The global nature of some businesses is a further challenge with third parties potentially located in different jurisdictions.

The industry representative summarized that operational resilience is about ensuring and maintaining trust and also about driving competitive advantage in the marketplace. This will require proportionality in the measures that are implemented and driving cultural change to ensure the changes are sustainable. The framework must be flexible because the threats, the technology and the operating environment are all constantly changing. It is therefore essential to have a mindset of integrated resilience involving all the stakeholders, including local and global supervisors and the industry.

The Chair agreed that there is a tension between taking a compliance approach and taking a spirit and principles approach. Achieving compliance is important, but implementing the spirit of DORA will be the key driver of positive outcomes.

2.2 Challenges for supervisors

A Central Bank official outlined the three main challenges for supervisors. The first challenge is the difficulty of coordinating the actions of the different authorities concerned by DORA at European and national level. Secondly, there is a scarcity of resources in the area of ICT risk. Regulators and supervisors will need to pool their resources in order to have sufficient expertise. Finally, DORA will impact supervisory activity. The oversight of CTPPs, for example, will require a specific approach due to the technical specificities of these providers and generate additional activity. Until now, supervisors have addressed these providers indirectly via the financial institutions using them, but they will now be supervising them directly.

A second Central Bank official highlighted three additional challenges for regulators and supervisors related to DORA. The first challenge is the timeframe. With only 15 months before the implementation deadline, national regulators must mobilise the existing knowledge in the relevant departments of their organisations to be able to quickly follow up on the recommendations of the DORA Joint Committee (JC). The second regulatory challenge relates to fragmentation. DORA is an unprecedented opportunity to implement consistent operational resilience rules across the financial sector. At national level, however, not all financial entities are regulated as financial institutions, such as leasing companies. To avoid fragmentation, DORA must cover all the entities performing financial activities. Thirdly, there is a need to update the existing methodologies and toolkits used to supervise ICT risk and monitor the impact of technology on business models. ICT risk will continue to be supervised according to the current rules until DORA is fully implemented. The improved understanding of ICT risk introduced by DORA will also need to be integrated into the overall supervisory view on banks' safety and soundness.

The Chair agreed that the practical realities of the implementation of DORA must be properly analysed. The EBA guidelines address some aspects of operational resilience, thus covering part of the scope of DORA, but the requirements will be extended to many different players and the rules will probably be less granular than what exists today.

A regulator noted that the purpose of DORA is not to repeal the EBA guidelines but to complement them. The EBA guidelines might be reconsidered at a future point in time.

The Central Bank official emphasised the importance of striking the right balance in the DORA requirements in terms of granularity. The framework should be technology neutral and not excessively detailed in order to adapt to future evolutions linked to technology. Supervision and regulation are mutually reinforcing and supervision can take over from regulation in areas where there have been new developments in the market or where regulation is not sufficiently precise. Supervision may also be faster and more effective than regulation for tackling certain issues.

2.3 The challenges posed by widespread or cross-border cyber attacks

A member of the audience commented that the nature of cyber and digital resilience will require supervisors to have a new mindset in addition to a new rulebook. With DORA, the Network and Information Security Directive (NIS2) and the upcoming Critical Entities Resilience Directive (CER), financial supervisors will be responsible for coordinating crisis management in the event of a widespread cyber-attack or failure, which could prove

to be challenging. On top of classical compliance-type supervision, supervisors will need to coordinate input and actions beyond the traditional sphere of ministries of finance, central banks and financial supervisors, across different government agencies.

A Central Bank official explained that cyber-attacks are already managed in a collective way due to the interdependencies involved. In each member state, different organisations bring the relevant stakeholders around a table with the supervisors. Usually, the central bank plays the leading role in this coordination, facilitating information exchange, ensuring the compatibility of individual actions and potentially steering the crisis management or recovery process. Supervisors already look beyond the impacts on individual financial institutions and take account of the collective consequences of any actions relating to business continuity or the remediation of a cyber-attack, therefore their role will not fundamentally change with DORA.

A second Central Bank official highlighted the cross border dimension of cyber risk. DORA is an attempt to ensure coordination within Europe, but the next question is how to improve the handling of these issues at the global level. The first step is to agree on a common taxonomy of incidents. The second is to simplify and unify the framework for incident reporting. There should be a single framework for incident reporting and greater convergence on the information that is shared in order to move fast in case an incident occurs. A balance must be struck between the sensitivity of sharing information and the need to have sufficient information to understand the bigger picture. Drawing a line between critical and non-critical incidents will also be important in determining a proportionate response to these events.

3. The CTPP oversight regime: objectives and challenges

3.1 Objectives and implementation timeframe

A regulator emphasised that implementing the CTPP oversight regime will be a significant challenge due to the tight timeframe and the extent of structural change needed. The Level 1 text contains a number of indications about the oversight process, but further specification is required in many areas. The new oversight regime is due to be implemented in 2025, even if the details are not entirely finalised by that date, which means that the CTPPs and their lead overseers will need to be designated in early 2025. Fees will need to be collected during that period to ensure that supervisors have sufficient resources to constitute their supervisory teams. The ESAs and the other competent authorities will need to start engaging with CTPPs and financial entities in 2024. TPPs can also opt in to the new oversight regime, which could make the process more efficient for all parties.

The Joint Examination Teams (JETs) will be the critical element in CTPP oversight. JETs will be the main tool of the lead authority overseeing each CTPP. The Level 1 text describes their potential structure. While one of the ESAs will be responsible for leading the oversight of a particular CTPP, in practice, the work will be conducted by a joint team, including the relevant competent authorities from the financial sector and other areas. Operationalising the process will require a full oversight cycle, going from the initial identification of the CTPPs and related authorities to the oversight itself and then to the remediation and the follow up on that remediation.

While this oversight approach is new and complex, supervisors are not starting from zero. Banking supervisors have expertise in operational resilience and experience of checking the adequacy of services provided by TPPs. The Single Supervisory Mechanism (SSM) teams also conduct on site inspections at banks to check the adequacy of their arrangements with TPPs. Indeed, the EBA outsourcing guidelines were groundbreaking in this regard. They showed banks and supervisors how to think about these issues. Additionally, the ESAs are already engaging with authorities from other jurisdictions. Over recent months, considerable effort has been made to learn what other authorities are doing and to think about how to achieve consistency and interoperability between authorities.

A Central Bank official agreed that the oversight regime for CTPPs will be an important evolution of the regulatory and supervisory framework, requiring an appropriate preparation with the different stakeholders concerned. CTPPs are not limited to cloud service providers (CSPs) and can be found in a variety of activities. The criteria used to define the list of CTPPs will be very important. These criteria will be both quantitative and qualitative, and defining these will require expert judgment.

3.2 Questions and challenges posed by the CTPP oversight regime

A Central Bank official observed that setting up the oversight of CTPPs will be a significant endeavour. First, determining which entities are CTPPs will be challenging. Italy conducted a first mapping of CTPPs two years ago. This process indicated that there were a significant amount of both IT and non IT CTPPs. In addition, the degree of interconnection in the financial market makes it difficult to draw the line between critical and non-critical entities. Criticality is not necessarily a question of size.

Secondly, there must be greater clarity on the precise roles of the lead overseer and the national competent authorities (NCAs). Implementing appropriate governance will be crucial for the success of the oversight framework. The JETs in charge of the oversight of CTPPs will operate alongside the existing Joint Supervisory Teams (JSTs) and Joint Oversight Teams (JOTs). This approach works in the SSM context, because its governance rules stipulate that the European Central Bank (ECB) takes the lead in the event of conflict. This will be more difficult to manage for the JETs because they are a form of cooperation between supervisory entities operating in different areas and sectors.

Thirdly, with the development of platformisation, the traditional concept of third parties might need to be

re evaluated, the Central Bank official observed. A CTPP might be the 'main player' in an ecosystem, and not a simple TPP, particularly if it serves smaller banks. In some cases, banks could be considered as the byproduct or front end of a larger platform offering data and analytics. These evolutions may require changes in terms of supervisory approach.

An industry speaker highlighted several key questions regarding the future CTPP oversight framework. First, this is a relatively new approach for supervisors. It is important for supervisors and the entities potentially concerned such as CSPs that are not supervised at present, to get to know each other. As the CTPP oversight framework is designed and implemented, it will be important to continue this dialogue. Secondly, overseeing these new types of entities will have new implications for supervisors. Supervisory practices will need to adapt to a new operating environment where innovation is continuous and largely driven by technology. For CTPPs that do not operate like financial entities it is necessary to define precisely how supervision will work in practice and how it may impact their activities and business models. For example, CSPs and their customers, which include financial institutions and governments, have concerns around the process that will be used for sharing highly sensitive information with the supervisory authorities. A further aspect to consider is that the financial industry is still at an early stage on its journey to adopt cloud computing. The regulatory and oversight framework should strike the right balance between supporting the adoption of this new technology, which has significant potential in terms of efficiency and resilience, and managing the related risks. This requires a regular dialogue between supervisors and the industry and also upskilling efforts within the supervisory authorities. The potential benefit of using technology to support regulatory and supervisory activities should also be evaluated.

A regulator commented that both supervisors and financial entities are in the business of handling confidential and sensitive data. The need for adequate data-sharing arrangements is a priority shared by all of the stakeholders concerned.

A second Central Bank official stated that supervisors are conscious that the process of oversight will need to be adapted to new entities and to evolutions happening in the market. The successful oversight of CTPPs will require close monitoring, potentially involving on site inspections similar to those carried out for financial intermediaries. The details have not yet been decided, but it is important for CTPPs to be prepared for this type of dialogue. The functioning and tailoring of the JETs will be an organisational challenge for the authorities. Regulators and supervisors should ensure that the priorities of the JETs are set correctly, building on their common experience, and that these teams have the right competencies and flexibility to perform their task. The functioning of these teams will probably evolve over time, which also needs considering. This cannot be embedded in a regulation but must be managed according to practice.