Digital operational and cyber-resilience: expected impacts of DORA and pending issues

1. Objectives of DORA and progress made with the legislative process

1.1 An increased focus on information and communication technology (ICT) and cyber risks

A Central Bank official highlighted that ICT and cyber risks have attracted increased attention from the financial industry and regulators in recent years. After the financial crisis, the focus was on financial and market risks and less on cyber risks and operational risks, but this situation is changing. Covid led to an increase in remote working and an expansion of digitalisation. As part of that process, outsourcing to ICT service providers, including cloud service providers (CSPs), has increased. Geopolitical tensions are also exacerbating cyber risks. As yet, there has been no major incident in the financial industry in the EU as a consequence of ICT and cyber risks, but that is not a guarantee that such a risk will not materialise in the future.

A public representative emphasised that recent geopolitical events, particularly the invasion of Ukraine, demonstrate how important cybersecurity is. Investment is needed, both from the industry and supervisors, to ensure that sufficient capability and competencies are available to tackle these risks. However, ensuring that the necessary resources are available will be a significant challenge.

An industry representative commented that the banking industry is a mirror of the economies that it serves and is dependent on the confidence of its customers. In the 80s and 90s, the biggest problems in the financial sector were due to credit and liquidity issues. These problems still exist, but IT and operational resilience risks have now become major potential threats. Banks have to operate as electric utilities nowadays, working permanently and with no outages to support an increasingly digitalised society and economy with operational financial and payment services. This involves processing tens of millions of transactions every day. Extremely high standards of operational resilience, mostly meaning technological resilience, are therefore needed. This involves a regulatory response as well as industry-driven initiatives. Although maturity and sophistication in the way financial services companies address ICT risks is increasing all the time, the pace of innovation and the range of issues that may go wrong increase just as fast. This is an area where it is easy to fall behind, which provides impetus to keep investing. Most financial firms are taking ICT and cyber risks very seriously. The smooth and effective responses by the financial industry to stress situations, such as Covid and the invasion of Ukraine, are also encouraging.

1.2 Progress made with the adoption of DORA and next steps

A Central Bank official stated that the EU DORA regulation (Digital Operational Resilience Act), aims to streamline the rules around ICT, third-party risk management, cyber-resilience testing and incident reporting. DORA also provides an oversight framework for non-financial critical third-party service providers (CTPPs) to the financial sector, which is a novelty.

A public representative emphasized the importance of cybersecurity which is being demonstrated once more in the context of the Russia-Ukraine war. There has been a great deal of engagement between the EU public authorities and many stakeholders in the elaboration of the DORA proposals, which have now been adopted. Guiding principles embedded in the drafting of the legislation include proportionality, future proofing and ensuring that Europe remains competitive and that innovation, creativity and R&D are not stifled as a result of DORA. DORA is therefore a balanced piece of legislation. Following the provisional agreement reached in May 2022 between the Council and the European Parliament, DORA will come to the plenary session of the European Parliament by November 2022. There will then be a two-year lead-in period for implementation. By late 2024 or early 2025, DORA requirements will become mandatory for all entities in its scope. It is hoped that there will be proper dialogue and discussion between the overseers and industry during this process, which will be a learning curve for both.

Responding to a question from the chair about the main areas of concern that have been tackled to achieve a compromise on DORA, the public representative commented that a first objective at the outset of the negotiations with the Council was to avoid a fragmented system, with different national competent authorities (NCAs) in charge of the oversight and different interpretations of the requirements. A reasonable compromise was found in terms of the oversight framework in particular, which should allow a consistent implementation of rules across the EU. Measures concerning CTPPs took up the largest portion of the time spent on discussing the legislation. Cloud outsourcing in particular has become an integral part of financial services and will continue to grow. A proper oversight of CTPPs, which are a limited number of massive global companies, such as CSPs operating globally, is clearly needed. The larger financial institutions can deal with major CSPs on a one-to-one basis, but smaller financial entities may not be able to. The aim is to ensure a level playing field in dealing with CTPPs for all types of financial players, so that the smaller ones are not disadvantaged.

A capacity for supervision to reach out into cloud services is also needed to ensure that there is integrity in the provision of these services, the public representative added. Cybersecurity is becoming a more prevalent concern and this is due to continue in the future. While it is widely accepted that cloud computing supports innovation and helps to improve customer service, it is also important to ensure that it does not create additional vulnerabilities in the financial system. The work on the Level 2 of DORA should aim at providing a clear and concise set of requirements that will allow a fast and compliant implementation, so that the financial industry can continue to innovate and improve customer service leveraging new technologies, while responding to its obligations in terms of security.

An industry representative agreed that achieving a minimum level playing field in how DORA applies across the financial sector is vital, because the sector is very interconnected and the overall system is only as strong as its weakest link. Level 2 standards must be promulgated quickly in a way that is implementable and enables progress. Standards should set a number of principles and minimum requirements as a safety net, because the detail of how to be optimally resilient will change all the time. Financial institutions should be able to set their own detailed standards of service and technological resilience in line with these principles and requirements.

1.3 Improvements expected from DORA

A regulator commented that DORA coming into force will be a significant achievement, even though there is still work to be done at Level 2. Standards already exist for addressing ICT and operational risks, but they are implemented differently across the EU which creates difficulties both for industry players and supervisors. Having a comprehensive framework for the entire European market with DORA will contribute to strengthening the resilience of the European financial sector. Three key features of DORA are to be highlighted. First, DORA provides an improved and harmonised framework for testing, which is essential. It is only possible to assess how resilient a system is by testing it. The testing needs to be thorough enough, identifying weaknesses that can be learned from. Secondly, it is welcome that DORA will be a lex specialis regulation, which means that it will prevail over more general rules, for example concerning reporting. This will help to streamline reporting and reduce the burden for the industry. Finally, the direct oversight of CTPPs will contribute to strengthening the supervision of ICT and operational risks in the financial sector. At present, the risks posed by CSPs are addressed by general oversight rules, which means that it is difficult to have a proper view of these risks, particularly when outsourcing to CSPs happens after several steps of outsourcing by different entities.

An industry representative stated that their company, a major CSP that services many European financial services organisations, shares the objectives of regulators on DORA. Achieving a high level of operational resilience and security is a key focus of their company as it helps to build confidence and trust in the cloud outsourcing operations they provide. Customers should be able to use cloud services in a secure way at all times and financial stability should also be guaranteed at market level. In addition, DORA is a major opportunity for harmonisation. Despite the EU level outsourcing rules established by the European Supervisory Authorities (ESA), there is significant fragmentation at the frontline level of supervision at present, creating obstacles for customers when they move to third-party providers. DORA should also help to create more transparency and trust by establishing a direct communication channel between third-party providers and the financial services supervisors.

A regulator commented that DORA will also provide significant benefits for regulated financial firms, allowing them to benefit from a more secure and harmonised framework instead of the existing fragmented approach, which will also contribute to reducing their regulatory costs.

2. DORA implementation challenges

2.1 Challenges faced by CSPs and different types of financial institutions

A Central Bank official commented that DORA will be successful if it is beneficial both to the public and to the private sectors. In answer to a question about potential concerns around implementation, an industry representative noted that Level 2 standards need to be brought out as soon as possible. Huge amounts of time and money are spent by the financial industry on digitalisation efforts and it would be extremely undesirable if part of that was wasted because players start moving in a direction that turns out to be incompatible with Level 2 standards or if they need to defer improvements because of delays in the publication of Level 2 standards. A second issue concerns the way proportionality is implemented. Experience as a practitioner over many years suggests that many cyber scares experienced in recent years are due to third-party suppliers involved in the process, rather than to the banks themselves. The regulation of third parties is therefore a crucial element of digital resilience. This is however challenging because not all of these suppliers are global players with a high level of professionalism. Proportionality is justified in the application of rules, but that should not lead to having a weak flank with some smaller providers.

A regulator noted that, for the largest banks and insurance companies, DORA will not constitute a real revolution, because these institutions are already subject to the existing guidelines drafted by the ESAs for the management of ICT and outsourcing risks, which constitute the core of the new DORA framework. DORA will however increase the level of harmonisation across Europe, requiring all institutions covered by DORA to reassess their practices and internal procedures and identify necessary adjustments, for example concerning the new European templates for information sharing. The time period for transition is also relatively short with a final deadline for 2025, which is a challenge. For the

financial and non-financial entities that are not already covered by digital operational requirements, such as the credit rating agencies or the insurance intermediaries, DORA will create a true shift of expectations in terms of practices and procedures. The proportionality embedded in DORA should however facilitate this process. The scarcity of skills in ICT risk management is also a key challenge for the private sector.

An industry representative noted that the main CSPs have been engaged with the co-legislators from an early point in the legislative process. This dialogue allowed the tackling of many issues, including those related to the proposal in DORA to move towards a pan-European, centralised approach to the oversight of CSPs considered as CTPPs. This is quite a new approach, since financial service supervisors will be overseeing technology companies for the first time and CSPs will be subject to a comprehensive oversight framework also for the first time. This creates a potential skills gap on both the supervisor and the CSP side. The industry representative's firm, a major CSP, is currently very focused on operationalising this new oversight approach with dedicated teams preparing for compliance with DORA. DORA is expected to have direct impacts on entities such as CSPs coming into direct oversight by the regulator, but also indirect impacts on how such entities will support new requirements for customers under DORA in the future.

The industry speaker added that while DORA is a technology-neutral proposal, it will primarily apply to cloud services in the first instance, so the specificities of cloud outsourcing, such as the multitenancy nature of these services, need to be appropriately taken into account in the requirements. All customers, financial and non-financial, are serviced from the same infrastructure. This means that the recommendations made by a financial services supervisor under DORA, e.g. around security or privacy protocols, will have to be implemented for all customers. In addition, during audits, a data centre cannot be switched off to test resiliency for one customer, because this will impact all customers.

2.2 Challenges for supervisors

A Central Bank official noted that the chairs of the ESAs had written a letter in 2021 expressing concerns about the practical implementation of DORA and making proposals about the oversight framework for CTPPs and the application of the proportionality principle in DORA, and asked what the main challenges for supervisors are expected to be.

A regulator confirmed that the implementation of DORA is a big challenge for supervisors. The three ESAs (EIPOA, ESMA and EBA) have been provided with some resources to address this challenge, but considering the workload, resources will still be very limited. The ESAs are working together on the implementation of DORA, sharing their knowledge, together with the European Systemic Risk Board (ESRB) and the Commission and also liaising with other authorities involved in ICT risk management. Existing guidelines that have already been produced in this area are being considered in order to avoid overlaps. There is an opportunity to deliver as a group on the oversight mandate, provided certain issues are considered. First, the timing is tight, so knowledge will need to be built progressively, which will also help to keep up to date with developments. Secondly, the approach to Level 2 requirements should be realistic, explaining the limits of the oversight that can be implemented and setting out what can be expected. A clear overview of how the governance system is expected to work is needed in the Level 2 requirements. It must be ensured that supervision adds sufficient value and is lean enough. A third issue is the availability of resources. 30 full-time equivalents (FTEs) are going to carry out the supervisory work at the European level, so prioritisation will be necessary. Finally, there is a need to train people. The help of the Commission in this regard is very welcome with the creation of a digital academy for supervisors. Experts from the market will also be sought.

Another regulator agreed that the public authorities will face challenges, in terms of resources and expertise, when providing supervision under DORA, which will cover a wide range of ICT services. DORA will involve all the supervisory authorities in charge of the financial supervision in Europe. All national and European authorities will therefore need to increase their competencies and expertise in the ICT risk field and pools of cybersecurity experts will need to be enriched. Where possible, resources that are already available should be used. The oversight of CTPPs is a particular challenge. The number of CTPPs is expected to be limited and the intensity of the oversight is meant to be adjusted strictly to need. However DORA will be a major innovation in this regard and a major project for the entire financial supervisory sphere in Europe.

The key condition of success is the adoption of collaborative approaches and lean management within the supervisory authorities, the regulator stressed. There are existing guidelines on ICT risk management and experiences in developing the single supervisory mechanism (SSM), the ESAs and the single resolution mechanism (SRM) should also be considered. There are already some resources and expertise in this area in the national competent authorities also. These competencies should be incorporated appropriately into the oversight framework. A system that can work as a single, smart and agile team across Europe will need to be implemented efficiently in a short period of time.

3. Consistency issues at the EU and global levels

3.1 Interactions across EU regulations

An industry representative noted that chapter V of DORA about the management of third-party ICT risk creates a significant overlap with existing outsourcing guidelines, which will need to be revised. How DORA will interact with other regulations addressing cyber-risk, such as the network and information systems (NIS) directive, also needs to be clarified. NIS creates a horizontal supervision that will apply inter alia to critical providers such as CSPs. There needs to be a precise cooperation of the

authorities under DORA and NIS. The final text resolves many of the issues of how cooperation will work in practice, but not all of them. There is also the question of how DORA will interact with forthcoming regulation, for example the Data Act. In addition, an EU cybersecurity scheme is under development, which will create a horizontal cyber framework applying potentially to financial players and CSPs in Europe, which is a further open question.

3.2 Global consistency of ICT risk management rules

An industry representative emphasized that global consistency is also very important in the area of ICT risk management. Sufficient European consistency should be ensured by the harmonised framework of DORA, the oversight framework of CTPPs and cooperation between the ESAs and the national competent authorities (NCAs), but DORA will regulate global technology providers and global financial firms together for the first time. There are similar trends in the APAC region and in the UK, with a proposal for a UK-style DORA under discussion. These elements need to come together to create a consistent framework. The Financial Stability Board (FSB) has a potential important role to play as a global standard setter in this regard.

A regulator highlighted the differences and similarities between DORA and the framework that exists in Switzerland. There are shared objectives in terms of operational resilience and tackling ICT risk events. There are three areas of focus in the Swiss framework when considering resilience of financial services companies, which are similar to those that can be found in DORA. The core requirement is that Swiss financial services companies need to map what they use, in terms of critical infrastructure systems, data applications and so forth, including their connectivity. The critical elements identified need to be shared with the supervisor so that a cross-sectoral view may be taken of where there may be reliance on common critical suppliers such as CSPs.

Secondly, operational risk management, in particular ICT risk management, needs to be integrated just like any other risk in the risk management practice. ICT risk must be recognised, mapped, analysed and mitigated and then monitored on an ongoing basis. Governance must also be clearly defined, i.e. who should decide on what, who does what and when. Effective governance is indeed essential in this space, particularly when it comes to dealing with incidents. Adequate supervision and inspection is also important. This requires planning and testing, but since it is not possible to test for everything that may happen in financial markets, there should be anticipation and scenario analyses carried out.

Thirdly, many of the issues related to digital operational and ICT risks are shared across the world and the industry. There is clearly a need for national and international cooperation, sharing of incident data and building up collective defences to cyber attackers. There is already a working level between the Swiss and the EU authorities on these issues, which should be continued and built on.

Finally, the regulator emphasized the importance of third-party risks. The fragmentation of supply chains is a natural way to create productivity by dividing up labour and this will not change. Therefore, it must be addressed from a risk management point of view. A useful principle from DORA, that is also applied in the Swiss framework, is technological neutrality. To the extent that the risks are the same, the same rules should apply. There is also a great deal of commonality on the more specific topic of outsourcing.