Cyber and digital operational resilience policy proposals

1. ICT Risk Management

1.1 Objectives of DORA in terms of ICT risk management and related opportunities

Introducing the discussion on the ICT[1] risk management measures of the EU DORA[2] proposal, the Chair described how, internationally and at a European level, the current financial regulatory framework for cyber and digital operational resilience is fragmented, extending across multiple binding and non binding standards which themselves vary between different sectors and jurisdictions. With DORA there is an objective to make these fragmented elements work together at the European level and create a reference point for tackling these issues. The trilogue process on DORA between the Commission, Parliament and the European Council have started. There are challenges around the proportionality of rules for different types of market players. There are questions also around whether or not DORA is future proof, i.e. whether it will be able to mitigate new and evolving ICT risks including cyber-risks. Having the necessary resources and competences for supervising these rules is also a challenge for supervisors.

A regulator considered ICT risk management to be a priority. 88% of respondents to a survey carried out by the European Banking Authority (EBA) among EU banks highlighted cyber risk as most prominent driver of increased operational risks in their organisations. In 2019 the EBA, with the other European Supervisory Agencies (ESAs), issued a recommendation to the Commission suggesting that this was an area where regulation should be enhanced, which is why progress on DORA is very much welcome.

Agreeing that one key goal of DORA is to establish a common framework for the management of ICT risks, a Central Bank official highlighted other main goals that DORA is pursuing: enhancing ICT risk management systems and frameworks within financial institutions, establishing the sound testing of ICT systems, increasing awareness about ICT risks within firms and public authorities, and also creating a consistent incident reporting mechanism.

A regulator agreed that DORA is an important step towards a more resilient European financial sector and a harmonisation of rules in this area. DORA is building on a solid but fragmented regulatory basis. The regulator was confident that DORA would allow significant progress, because it builds on the fundamental elements developed by the G7 on cybersecurity and the FSB work on response and recovery. These are the current best practices, however the question of their future-proofness remains relevant.

An industry speaker emphasised the opportunities represented by digitalisation in the financial sector. The EU is still in the early stages of its digital transformation, but the pandemic triggered a considerable acceleration of this transition, with five years' worth changes being achieved in a few weeks. While technology creates new opportunities for consumers, the bar needs to be raised in terms of security and resilience. Another industry representative agreed that DORA presents an opportunity to increase consistency across the EU by aligning rules and guidance in the area of cybersecurity and resilience and also creating a supervisory framework for assessing technology risks within and outside financial institutions.

1.2 Issues and challenges to further consider regarding DORA ICT risk management measures

1.2.1 Interaction and consistency with other regulations

A regulator noted the importance of better defining how DORA will interact with other parts of the regulatory framework at domestic and EU level, because there is significant complexity around this interaction. Almost all competent authorities are interacting with supervised entities on the improvement of their cyber risk capabilities. 11 EU member states have already adopted or are in the process of adopting the TIBER-EU framework (threat intelligence-based ethical red-teaming) for threat led penetration testing. There is moreover considerable work underway on the enhancement of sharing and collaboration between different authorities involved in ICT risk management i.e. financial sector and cross-sectoral authorities, domestic and cross border ones.

An industry representative stressed the importance of also considering in the trilogues, the interactions between DORA and ongoing regulatory activities at the international level, such as the BCBS principles for operational resilience (which include cybersecurity requirements) and also the FSB initiatives on third party and ICT risk management. The industry representative stated that there may be a few challenges that may exist with the current versions of the DORA text. The first issue is around impact tolerances. An impact tolerance is a measure which determines the point at which a disruption will impact financial stability or the viability of a firm. DORA and the BCBS use different approaches to this measure: while the BCBS views impact tolerance from a business operations perspective, DORA considers it in terms of technology. This may require the establishment of two different impact tolerance measures - one for business operations and one for the underlying technology – which could

1. ICT: information and communications technology
2. DORA: Digital Operational Resilience Act

create serious confusion. Secondly, cyber incident reporting requirements under DORA raise potential consistency issues with international rules. These include the conflation of definitions, such as 'cyber incident' and 'cyber event', which might create confusion when DORA is integrated into the larger global cyber incident reporting frameworks being developed.

A regulator observed that DORA should also be consistent with existing EU regulatory frameworks, such as the guidelines and regulations of the ESAs. In areas such as IT project management and application development, the ESA guidelines should complement and reinforce DORA requirements.

A Central Bank official suggested that it is necessary to make sure that the provisions in DORA will, in combination with existing regulatory measures, make European firms sufficiently resilient to continue delivering their critical functions during disruptions. This will have to be assessed during the implementation of these measures through collaboration between the authorities and firms.

1.2.2 Implementation challenges

A Central Bank official noted that the differences across banks in terms of maturity on ICT risk management will make the implementation of DORA quite challenging for firms and authorities. These differences in maturity stem from the complexity of the organisations, their IT systems or the way pre-existing EBA guidelines on ICT security risk and outsourcing have been implemented. Implementing DORA will require some firms to make a significant effort. This will also be challenging for the authorities due to a potential lack of skills and resources, particularly for supervising the more sophisticated financial institutions in this area.

An industry representative explained that DORA is seen positively in terms of harmonisation by many financial institutions. Nevertheless, firms want more clarity on the precise and detailed implementation steps which they are expected to make. Another industry speaker suggested that firms would need time to prepare for DORA, because they will need to develop the necessary skills and will also have to build applications to address cybersecurity and resiliency issues with proper architectures.

1.2.3 Proportionality issues

A Central Bank official emphasised the importance of ensuring an appropriate level of proportionality in DORA for each type of institution depending on its complexity. Firms and supervisors will need to discuss this in greater detail. There is a desire to raise the bar here, because digital operational resilience is crucial for the resilience of the EU financial sector, but it is important to find the right balance.

A regulator agreed on the importance of ensuring the bar is raised on digital operational resilience and kept high. When applying the principle of proportionality, especially in the context of cyber-resilience, it is important not to reduce the ambition too much, but ensure that a minimum level of cyber hygiene is implemented by all market players.

1.2.4 Information sharing

A Central Bank official considered information sharing to be another important objective. DORA will mandate the authorities to share information between each other. This is a challenge, because this sharing will occur not only between financial supervisory authorities but also with cross-sectoral supervisory authorities. But enhancing cross sector cooperation and building up EU cyber intelligence is essential for enhancing resilience since cyber-incidents can propagate very rapidly across entities of different sectors.

A regulator agreed that there are significant challenges around information sharing and collaboration. It is of tremendous importance that in times of crisis or stress in particular, there is secure and timely information and that best use is made of European resources and knowledge in the field of cyber-resilience. Information sharing and collaboration is of utmost importance in this regard and needs to be enhanced. The supervisory landscape drawn by DORA and existing initiatives contains a large number of components that need to be coordinated in an appropriate way. These include threat led penetration testing; Threat Intelligence based Ethical Red Teaming (TIBER) and the dedicated TIBER community; the oversight architecture, with dedicated joint oversight teams working on incidents reported to supervisors and more traditional teams carrying out on site inspections at financial institutions; the Network Information Systems Directive (NIS) ecosystem; and the Cyber Security Incident Response Teams (CSIRTs).

1.2.5 Future proofing

The Chair asked panellists whether DORA would be able to create sufficient resilience in the future, given the progress and innovation happening on digitalisation, cyber risk and service provision. A question is whether there is the appropriate balance in DORA between a principles-based and a rules-based approach to tackle present risks and those that may emerge in the future. Another is what should be the process for updating DORA to reflect new challenges and progress made on digital operational resilience.

An industry representative noted that the same principles have been used to address cyber risk for decades, but the detail of the framework may have to change to reflect evolutions in the underlying technology and security architecture standards and how they are used. That should drive what is done at a more granular level. In terms of future-proofing, DORA must be sufficiently high level to allow the overall framework to be still valid when activities progress, which is unavoidable with new and emerging technologies, the evolution of which is impossible to predict.

Another industry speaker added that giving players sufficient time to implement and having adequate dialogue and coordination across the industry will be essential for futureproofing DORA, because it will give firms flexibility as the needs of the industry continue to change. Cybersecurity is not static, and neither are the industry's needs around resiliency.

2. Third-party provider ICT risks

2.1 The challenges of third-party vulnerabilities

An industry representative described how a survey conducted in 2021 among financial institutions in the UK indicated that third party vulnerabilities are seen as the most challenging aspect of operational resilience. Addressing the issues raised by dependency on third party providers (TPPs) is also a key priority for the management of these institutions. Based on the information available to date, it is however clear that many financial services firms have not yet ascertained how to address these vulnerabilities. DORA will likely have a 24 month implementation period, but the Level 2 regulatory technical standards will take much longer to finalise. Firms should not wait for the conclusion of this legislative process to address these new challenges, because timing is essential in this area. A certain number of 'no-regret' actions can be taken now by firms to start tackling third-party vulnerabilities. First, a gap analysis of the existing ICT risk framework can be conducted especially focusing on TPPs. Secondly, a holistic view of TPP connections can be developed in order to document and review the vulnerabilities arising from the use of TPPs. This can support the structuring or updating of a risk containment strategy. There are also questions in terms of international and group-level consistency. Cross border firms should start by implementing a standardised approach at a group wide level and then adjust to local regulation or specificity if needed. The Chair agreed that the financial sector is generally not well aware of all the risks concerning TPPs, which shows that there is a need for DORA to be implemented quickly to tackle these issues.

2.2 DORA objectives regarding the supervision of critical third-party ICT providers (CTPPs)

The Chair noted that third party ICT risks present many challenges, including the management of third party/fourth party risk and concentration risk. Handling these issues is one of the key objectives of DORA, which contains notably a new proposal concerning the oversight of critical third party service providers (CTPPs), including those based in third countries. However, it is essential to define precisely these terms, because oversight is different from supervision[3]. In addition, the DORA proposals concerning TPPs must be reconciled with the work of the FSB and IOSCO in this area, and also take into account the need to develop adequate supervisory capabilities.

A regulator explained that a basic principle driving DORA is the assumption that supervised financial entities are responsible for the risks that are created by their activities throughout the whole value chain, including TPPs. This can be difficult to manage for financial institutions, especially when some TPPs are major global players providing services to a large number of entities in the financial sector and potentially raising systemic issues, which is the underlying reason for the oversight of CTPPs mandated by DORA. The way in which TPP services are provided may evolve, as well as the TPP industry structure, but at this stage it is important to address potential concentration risk adequately. It is however important to understand what DORA does and does not do. DORA mandates an oversight and not a supervision of CTPPs. Additionally, this is an oversight of the provision of ICT services exclusively to the financial sector, not an oversight of the services provided by CTPPs across all industries. Thirdly, DORA will address the provision of ICT services by CTPPs across all financial activities such as banking, insurance services, securities markets and so on. A lead overseer will be identified for a given CTPP in charge of overseeing the provision of services by this CTPP across all financial activities.

Ensuring an appropriate interaction between the supervisor of the financial entity, the lead overseers of the relevant CTPPs and the other competent authorities concerned will be quite challenging, the regulator felt, and needs to be defined in the context of the implementation of DORA. In addition, there is a question of enforcement of supervisory measures concerning TPPs. At present, supervisory decisions concerning TPPs (e.g. the request to change providers or to modify the way the services are delivered) are imposed on the supervised financial entities, but that is quite an indirect process. With DORA, these requests could be addressed to the supervised financial entity or to the CTPP. It would be probably more effective to go directly from the lead overseer to the CTPP, rather than through the supervisor of the financial entity, but this needs to be clarified. It is also important to understand which supervisory entity will be in charge of requesting changes. This could be the supervisor of the supervised financial entity or the lead overseer of the CTPP.

A second regulator supported the implementation of a European level oversight for CTPPs, which will allow having a counterweight against large global service providers that have developed a strong footprint at the European level. The success of DORA in this regard will however depend on the criteria established for identifying CTPPs and defining how they should be overseen.

The Chair agreed that there are many issues remaining to be tackled regarding the implementation of DORA. Supervised financial entities cannot be made responsible for their TPPs in all circumstances, particularly when TPPs are much larger than the supervised entity, which in that case has little real power to request changes. A Central Bank official agreed that this is a question of power as well as proportionality. A global TPP has a power that is very significant and this needs to be taken into account. A first key step is the designation of the CTPPs to be supervised, which will also be crucial for preparing the implementation of DORA, because it will help to determine the skills and resources that the authorities and also the TPPs will need for implementing the legislation in a context where these are in limited supply.

An industry representative noted that, as a result of DORA, cloud service providers (CSP) in particular will

3. Oversight is considered less intrusive than supervision. Oversight might be viewed more as surveillance, i.e. conducted at a distance, while supervision involves close first-hand observation and analysis and direct interaction with concerned entities on a regular basis.

most likely be placed under the direct oversight of the European Supervisory Authorities for their activities in the financial sector. This will bring new third parties and non financial services firms into the scope covered by financial services supervisors. However, this will require the building up of new skills within the supervisory authorities to address cybersecurity issues and risks related to cloud usage, which is quite challenging given that resources are scarce in these areas. This will require preparation and anticipation.

Another industry speaker acknowledged that while CSPs are not sources of risk per se, there is a need to ensure adequate cybersecurity and resiliency across the different actors operating in the financial value chain, including CSPs. The most encouraging element of the debate on DORA is the objective to increase the harmonisation of rules, because the policy approach to outsourcing is quite fragmented at present. If DORA can harmonise the approach to TPPs, it will allow participants, providers and regulatory organisations to have common understanding and expectations, which will facilitate the implementation of requirements and lead to higher resiliency and security. Implementing fragmented requirements can be challenging for international financial institutions, because it requires them to create their own holistic framework incorporating the different existing rules. DORA therefore represents an opportunity to create the harmonisation that will facilitate this approach.

2.3 International consistency questions related to TPP DORA measures

An industry representative emphasised the importance of ensuring consistency between DORA and the BCBS principles for operational resilience concerning TPPs. First, regarding intra group ICT providers, more proportionate rules would be needed, because DORA considers them in the same way as external TPPs. This does not seem appropriate, since there are differences in terms of risk profile, e.g. there can be more confidence in the management of risks by a sister entity if similar processes and tools are in place. In addition, exit strategies (i.e. the strategy used by the financial institution to offboard a TPP) also have different implications for intra-group TPPs and external ones. The impact of a change concerning an intra group ICT provider will indeed be much more significant for the organisation, because it might not only affect ICT services, but also the intra-group management of Compliance, Risk (including cyber risk) or HR. Additionally in many cases an exit strategy for an intra group provider will not be implemented in practice, because it is not feasible to implement it in a way that does not 'kill off' an affiliate whose financial health is largely based on that of its parent. There are also potential issues around contractual terms, such as the obligation for a parent organisation to provide assistance to affiliate entities for ICT incidents, given the reputational or safety implications.

A second issue around TPPs in terms of consistency with BCBS requirements, the industry speaker noted, is the level of granularity required in DORA around the mapping of interconnections. The main concepts and tools used by DORA and the BCBS are similar such as process mapping, impact tolerances and an understanding of third party dependencies. However, the scope of the mapping in DORA is more extensive. The aim of the BCBS principles around the mapping of interconnections is to ensure that financial entities understand how their functions and business operations fit together with TPPs and to enable them to define how they will respond in case of problem based on different scenarios. DORA, extends that mapping into system configurations, which means that it may need to be updated each time a system is patched or upgraded, potentially mobilising significant time and resources.

Referring to the comments about intra-group providers, a regulator added that the ability of a supervisor to enforce supervisory measures is different for an intra-group entity of a regulated financial entity and for an external provider. A large amount of ICT services that were previously sub-contracted to intra-group or specialized entities of financial groups have however been shifted to external players, some of which are now very large players at the international level. This is where the proportionality argument has emerged mainly in the DORA discussions.