DIGITAL OPERATIONAL AND CYBER-RESILIENCE
(DORA, NIS)

1. Objectives and status of the DORA proposal on ICT risk management

The Chair explained that research from the Global Domain Name System (DNS) Threat Report had revealed that nine out of 10 companies worldwide were victims of a cyberattack in the previous year, showing the importance of the issues addressed by the EU Digital Operations Resilience Act (DORA) legislation. The legislative process concerning the DORA proposal and involving the Parliament and the Council is underway. Digital innovation fundamentally changes banks' and other financial institutions' business models. This has the potential to make them more competitive and profitable. However, it also makes them more vulnerable to information and communications technology (ICT) risks, be it on premise or related to third-party providers.

An industry representative gave an idea of the magnitude of cyberthreats threatening society at present and of related reporting challenges. In 2020, their company, a major tech company, blocked close to 6 billion malware threats on endpoints controlled by their system. This is not only in finance and is a global figure, but it is a figure for only one tech company and shows the importance of the problem that needs to be addressed.

A public representative explained that the European Commission published the DORA proposal last November 2020. In March, a draft report was published by the rapporteur and there are now discussions within the European Parliament's ECON Committee to arrive at a consensus. DORA is an ambitious proposal which is important for ensuring the integrity of financial services faced with significant threats in terms of cybersecurity. DORA aims to ensure that there is built-in integrity in the financial system, setting a benchmark at the international level in this field, and also aims to increase uniformity in the EU policy approach, undoing the current patchwork of guidelines, regulation and oversight at member-state level.

The guiding principles of DORA are proportionality, future-proofing and competitiveness, the public representative added. The desire is to ensure there are proper guidelines, oversight and regulation in place, which are also fair, reasonable and proportionate, in order to avoid overburdening the industry and supervisory authorities. In terms of future-proofing, financial services now live in quite a dynamic space with the increasing use of cloud-computing and ICT, and new technologies are continually evolving. The objective is for the financial industry to be able to adapt to these evolutions and benefit from future innovations in a safe way and for the area of cyber-resilience to be future-proofed and flexible.

An industry representative stated that digitalisation provides many benefits within the financial services industry, contributing to extend financial services to excluded or underserved individuals, enhancing customer experience, increasing efficiency and leading to lower transactional costs. These benefits are enhanced through the interconnectedness of the financial markets, but that increases reliance on the digital infrastructure used to deliver financial services. DORA aims to provide a cohesive approach to cyber-resilience across the EU, recognising that independent national approaches to this cross-border risk will limit the effectiveness of financial institutions and authorities to deliver on their resilience objectives. Concerning financial market infrastructures, DORA is aligned with CPMI-IOSCO cyber-resilience guidelines.

Another industry representative explained that until recently cybersecurity was only a minor item in regulation. Only in 2017 were the Supervisory Review and Evaluation Process (SREP) guidelines of the EBA updated to include a meaningful section on cybersecurity. DORA is aiming to address some of the inevitable consequences of the rapid speed of regulatory change that has been taking place within the EU and the industry representative agreed with the objectives set out including proportionality, future-proofing and innovation. If done well this will result in more resilient and more innovative financial services. Future proofing is particularly important because cyber-risk is changing so rapidly that firms must have the ability to adapt equally as quickly or risk becoming victims.

2. Potential areas of improvement of the ICT risk mitigation provisions of DORA

2.1 Future-proofing, proportionality and flexibility

An industry representative noted that, as a Level 1 text, DORA provides an outline that will ultimately need to be specified by the European supervisory authorities (ESA) and the European Union Agency for Cybersecurity (ENISA) for its implementation across the EU. A balance needs to be struck between being prescriptive in certain approaches in order to provide sufficient guidance, and allowing for sufficient flexibility to cover a broad range of financial institutions. It is important that the regulatory technical standards (RTS) outlined in the Level 2 text should be created in partnership with financial institutions to ensure that proportionality is maintained.

Another industry representative stated that future-proofing DORA can be best achieved by avoiding technical prescription and focusing on outcomes. For example, legislation should not prescribe how a firm achieves its data recovery in the event of a data integrity incident. Prescriptive rules could limit firms' ability to quickly adapt their strategy as technology changes. Future-proofing and granting firms that flexibility also results in a much greater proportionality, since it allows firms to make decisions that fit their risk profile.

The Chair noted that proportionality is also needed in the way supervisory tasks are carried out with a risk-oriented approach. Bearing this in mind, proportionality will be an important aim when developing the regulatory standards for implementing the DORA rules. A regulator emphasised that one size does not fit all in this context. Supervisors have a very positive view of the DORA proposal. The measures included are fit for purpose, but it is key that they remain proportionate because there is a wide variety of entities in the scope of DORA and many dimensions to cover. Implementing DORA will also require significant efforts from financial entities and the supervisory community given the number of requirements. Technical standards will be developed in conjunction with the financial entities that will have to implement them, but the diversity of entities in scope needs to be taken into account along with their digital maturity.

EIOPA welcomes the introduction of proportionate provisions in DORA and the recommendations of the Parliament report going in this direction. The DORA regulation should allow proportionality as a general principle. The goal is to have an overarching proportionality principle applied to the full DORA regulation, so that in the future there is no doubt that proportionality still applies, even if it is not referred to in specific articles or if specific exemptions do not exist.

EIOPA's remit covers insurance companies, insurance intermediaries and institutions for occupational retirement provision (IORP) and there are very different situations there. Insurance companies are already subject to a certain number of requirements in the area of ICT risk management, thanks to Solvency II and the recent EIOPA guidelines on ICT and on outsourcing to the cloud, which will facilitate the implementation of DORA, although new developments will be needed in the areas of incident reporting and testing. The situation is completely different for intermediaries or IORPs, for which the implementation of DORA will require significant efforts, to be balanced with a proper application of the proportionality principle. Intermediaries need to be considered differently from big insurance companies or banks, the regulator suggested, but exclusion should be based on risks in line with the resiliency objectives of DORA rather than on the small size of intermediaries. If intermediaries conduct business and insurance-distribution activities on behalf of insurance undertakings covered by DORA, they will be provided with adequate network and information systems, and the security of these systems will be the responsibility of one or more entities under the scope of DORA.

In addition to this, the supervisory authorities at both the European and national levels should consider how to approach operational resilience risk related to digitalisation for entities excluded from DORA, possibly with simpler national approaches, because these entities should not be allowed to become weak links within the financial system. Proportionality might also require different implementation timelines, with larger transitional periods for smaller entities, for example the regulator stated.

2.2 Incident reporting

An industry representative suggested that there should be a greater alignment of DORA with the ongoing global cyber-resilience initiatives in areas such as incident reporting. The recent spate of ransomware attacks has increased the focus on this area. Foundational to any cyber-incident reporting is terminology and how cyber events and cyber incidents are defined. The original DORA text introduced a new term, 'major ICT-related incident', which may further fragment what is required for financial institutions to report. A 2021 IIF staff paper on the importance of more effective cyber-risk reporting highlights some of the challenges faced by financial institutions in this area, and potential policy solutions that may offer insights to help build the DORA cyber-incident-reporting framework in a consistent way.

Another industry representative agreed with the importance of aligning DORA's incident reporting requirements to forthcoming global standards from the FSB. The industry representative also suggested that policy attention should start shifting away from the collection of large quantities of information to how that information is analysed and redistributed as intelligence into the industry. Intelligence from authorities should aim to help firms to identify what to look for in their systems e.g. IP addresses to track or signatures in malware. There are improvements that can be made in that field that will outweigh what can be done by collecting even more information. For example cyberthreat notification does not seem to add much value. An excessive provision of information may increase cybersecurity risk when that information is highly sensitive, the industry representative stressed. Several points in DORA (e.g. Art. 13) include requirements for firms to reveal information on vulnerabilities, either publicly or to clients, but revealing its vulnerabilities may increase risks for a firm while providing little practical benefit to end users. That simply makes it more likely that those vulnerabilities will be exploited and so it creates significantly more risk. Supervisors should continue to instead push financial entities to reduce the amount of time it takes between identifying a vulnerability and patching it.

2.3 Threat-led penetration testing

An industry representative suggested that threat-led penetration testing is another area that requires further optimisation. It requires strong intelligence and specialised experts to execute. The European Central Bank (ECB) Threat Intelligence-Based Ethical Red Teaming (TIBER) framework allows for member states to build bespoke threat-led penetration-testing requirements. Limited availability to experts in this space may however impact the ability for all in-scope financial institutions to execute such testing. Moreover, the requirement to have assessors certified per member state may impact the accessibility of these assessors for all financial institutions.

Regarding contractual obligations, financial institutions continue to rely on outsourcing and other third-party arrangements to deliver financial services. However, several challenges associated with these relationships were outlined in the 2020 Financial Stability Board's report relating to outsourcing and third-party relationships. For example, requiring ICT providers to participate in threat-led penetration testing may prove difficult for financial institutions to negotiate.

3. Issues and challenges raised by the ICT third-party provider provisions of DORA

A public representative noted that the role of third-party ICT providers has significantly evolved in the financial services sector compared to 10 years ago. They are now critical components of the sector and there is a whole range of providers in this space, which has to be regulated. Ensuring the reputational and operational integrity of financial services in Europe, requires addressing issues raised by third-party providers as well as by the providers of financial services. There had not yet been a formal discussion on the third-party provider part of DORA in the ECON Committee at the time of this panel discussion but a decision will be made on that particular issue in the near future in order to ensure that there is not an unbalance in terms of obligations between regulated financial entities and critical third-party providers (CTPP) subject to very different obligations.

3.1 Oversight regime for Critical Third-Party Service Providers (CTPP)

An industry representative stated, regarding the oversight regime for CTPPs proposed in DORA, that it is important to modernise regulation and provide a harmonised set of rules, because of the fast-moving pace of technology and its pan-European character, and DORA plays an important role in that. Cloud services in particular are a key driver of the digitalisation of different sectors including financial services, so it is quite natural for it to be part of this regulation. In terms of the scope of the oversight, it is currently foreseen that the identification of CTPPs will be carried out at the provider level, without distinguishing between the types of services offered by those providers, even though they can be quite different and do not all concern financial services. There should be more clarity on what the focus of the overseers should be. In terms of process, the Commission proposal was also relatively silent on what the interaction between the oversight authorities and the CTPPs should be, so there is a need for further clarity here.

Harmonisation is another issue, the industry representative emphasized. Given the dichotomy between the oversight authorities and the national competent authorities (NCAs), if DORA makes room for national fragmentation there will be problems in terms of compatibility and consistency of the requirements. There are also consistency issues between DORA and the Network and Information Security (NIS) Directive concerning resilience measures for CTPPs. If there are incompatible resilience recommendations, measures and obligations then it will not be possible for cloud service providers for example to implement them both.

A regulator stated that there are two important points for making the CTPP oversight framework effective and efficient. The first is having an adequate representation of different financial sectors, for which third-party providers are relevant. Therefore, the system of having potentially three lead overseers is important. Clear and balanced roles, responsibilities and powers between national and European authorities are also absolutely crucial. A joint ESA executive body, which will be small and functional, with proper technical capacity and expertise, and with limited membership from the European authorities and NCAs, is the right way forward, together with the establishment of cross-ESA teams to work on the oversight of CTPPs.

In addition it is important to consider how cross-ESA teams work, because there cannot be a patchwork of implementation. Currently, NCAs reassess the situation and may have different nuances concerning the lead overseer's recommendation on issues such as the level and maturity of non-compliance, but in this area there needs to be a European approach based on the recommendations of the lead supervisor and then a national implementation consistent with the findings of the lead overseer. The regulator highlighted Article 37 of DORA, where paragraph 4 in particular has to be correctly implemented. There needs to be flexibility from national supervisory authorities while focusing on the impact of the non-compliance of their supervised entities. This is the only way to have a European approach that is focused on specific supervised entities, without reassessing and giving different nuances to the assessment of the lead overseer.

Another regulator concurred that, under the present architecture, this is the right approach for moving forward. Convergence, cooperation and consistency are fundamental to having a proper way forward with respect to supervision in this area.

3.2 Concentration risk, location and sovereignty issues

An industry representative noted that DORA wants financial institutions to identify concentration risks with the major ICT providers they use. While this may be possible internally to their organisations, they cannot do this at market level because they do not have access to the data that would be needed to understand how other financial institutions are using their cloud service providers or other ICT providers. In addition, financial institutions often do not inform cloud providers or ICT providers of the services that they are running on their infrastructure, so the latter may not know whether or not they are running critical operations. These requirements therefore need to be further clarified both at Levels 1 and 2.

Answering a question from the Chair about the domestic or global dimension of cyber-resilience and the possible need for enhanced sovereignty in this area, an industry representative stated that policy-makers want to ensure they have the right to exercise authority over the providers in this area. However, unlike some traditional areas of financial services regulation such as capital requirements, technology operations do not easily fragment along national borders. Fragmentation in the technology estate of a financial institution creates more complexity, which creates an increased chance of failure, makes it harder to apply security controls across the entire estate and increases the attack surface that has to be defended.

Localisation and the accompanying fragmentation of technology operations creates real risks and barriers to the ability of financial entities to make their digital operations resilient, the industry speaker felt. One example of where DORA may contribute to localisation is Article 31. It is a challenge to work through how best to achieve the national resilience objectives that are

legitimately being sought by policy-makers without adding any increased technology or cyber risk through localisation requirements. Such requirements have even started to appear between member states and risk becoming a barrier to a single market within the EU. The natural tendency of assuming that proximity equals security has to be resisted and there has to be consideration of what outcomes are sought, what has to be done and how it can be achieved without adding cybersecurity or IT risk to the financial sector.

4. Adapting the supervisory approach and architecture to cross-sectoral risks such as cyber-security

The Chair noted that supervisors who traditionally focused on a specific financial sector are now being asked to apply multisectoral financial regulations such as DORA in a number of cases, which is more complex.

A regulator suggested that the main issue for supervisors is the interconnectedness within the financial system and the importance of having not only regulation that is harmonised with the introduction of DORA, but also consistency in the level of supervision. This raises a number of questions to be addressed by the MEPs currently considering the DORA proposal. One is whether there is the right architecture to allow a proper and consistent supervision of cyber risks within Europe. Another is if the current architecture at supranational level with a largely sectoral approach to financial supervision is correct. That should be considered particularly given the evolution of regulation, which is becoming more cross-sectoral, not only in the field of cyber risks but also in areas like sustainable finance, anti-money-laundering (AML) and combating the financing of terrorism (CFT).

DORA addresses the issue of the fragmentation of regulation with a single rulebook that regulates the area of cybersecurity. However, over 40 supervisors will be responsible for supervision in this field, which may create fragmentation, leading to possible supervisory gaps and system failures. That leads to another set of questions. One is whether the supervisory architecture should be considered at the national level and whether the NCAs will have sufficient human and technical resources to effectively supervise DORA. Another is what can be done at the supranational level in order to support the NCAs. It can also be asked how a degree of consistency can be ensured and if it should be more compliance-based or more outcomes-based. Just as there is a recommendation for the ESAs to look into setting up a central hub for incident reporting, there should be an invitation for them to assess the architecture of financial supervision and the resources that are needed at European and national level for achieving the objectives of DORA.

A public representative noted that it would be a catastrophic failure of public policy if a uniform regulation such as DORA was then being enforced and overseen in a patchwork fashion across the EU. The European Parliament is very conscious that there needs to be a sufficient degree of uniformity in the oversight across member states and that the proper oversight architecture needs to be put in place in order to achieve that. The adequate resources will also have to be put in place. In order to ensure effective reporting and an assessment of that information by the oversight bodies, the proper resources have to be in place, both in terms of sufficient capabilities and sufficient people on the ground, otherwise there will be significant difficulties.

Conclusion

The Chair summarised that it is critical for the DORA legislation to not hinder digital innovation or overburden the financial industry in Europe. Level 1 regulation should be technologically neutral and principle-based to allow quick adaptations to technical innovation. A sound institutional architecture is also crucial. The supervisory authorities should have clear-cut competencies in order to avoid overlaps or gaps. The importance of adopting a proportionate and risk-based approach, not only in the day-to-day oversight but also in the regulation, was also emphasized.