DIGITAL OPERATIONAL RESILIENCE ACT (DORA): MAIN PROPOSALS AND PENDING ISSUES

Note written by Marc Truchet, EUROFI

1. Objectives and context of the DORA proposal

In September 2020, the European Commission published the Digital Operational Resilience Act (DORA) proposal, which aims to ensure that financial institutions in the EU can support the continued provision of services and their quality, and thus preserve the stability of the EU financial system, in the event of any potential disruption or threat to operational resilience in relation to their use of information and communication technology (ICT).

Digitalisation and the use of technologies such as cloud computing, distributed ledger technology (DLT), artificial intelligence (AI), machine learning (ML) are progressing at a fast pace in the financial sector, making ICT risks such as cyber-attacks, system failures and other ICT-related incidents a focal point for regulators. In addition, potential risks stemming from the dependency of financial entities on ICT third-party service providers (such as providers of cloud services, software, data analytics and data centres), have been emphasized by regulators at the global and EU levels in a context of increasing outsourcing of activities and services to these providers, although no specific signs of fragility have been evidenced so far, notably throughout the Covid crisis, during which cloud services in particular supported business continuity.

In order to avoid major operational disruptions from these risks, DORA proposes to establish a comprehensive and harmonized framework for the management of ICT risks by financial institutions and also to introduce an oversight framework for third-party providers of ICT deemed 'critical' for the EU financial sector. DORA is part of a wider Digital Finance Package proposed by the European Commission, which seeks to support a further digitalisation of the EU financial sector in terms of innovation and competition, while mitigating the risks arising from it[1].

DORA also builds on a number of existing European policies and standards addressing ICT and outsourcing risks including the Network and Information Security (NIS) Directive[2] on cybersecurity currently under review, the TIBER-EU framework of the ECB[3] concerning voluntary penetration testing, the EBA ICT and security risk guidelines and the guidelines published by the European Supervisory Authorities (ESAs) for the outsourcing of cloud services. General operational resilience requirements are also embedded in the main financial regulations such as CRDIV, Solvency II, MiFID II and PSDII.

The combination of these different EU measures with international principles on operational resilience[4] and with national reporting and testing requirements[5], however results in overlaps and inconsistencies across jurisdictions, leading to the potential risk of regulatory fragmentation. The Commission is aiming to improve the consistency of these requirements with DORA, in order to support supervisory effectiveness of ICT risks in the financial sector and reduce the administrative and compliance burden for firms. The DORA framework will moreover apply to a wide range of entities (financial entities and intermediaries, infrastructures, service providers), in order to ensure consistency in the way ICT risk management is implemented across the financial sector.

1. The Digital Finance Package includes the Digital Finance Strategy (DFS), which aims to ensure that the EU financial sector and its customers embrace the digital revolution by improving the functioning of the Digital Single market for financial services, ensuring that EU financial regulation and supervision are fit for the digital age and establishing a common European financial data space to facilitate data sharing and promote data-driven innovation. The DFS is completed by four additional regulatory proposals covering different technologies and areas of digitalisation: MiCA (the regulation on Markets in Crypto-Assets), a pilot regime for DLT market infrastructures, DORA (the Digital Operational Resilience Act) and the EU Retail Payments Strategy.
2. The NIS Directive provides legal requirements and best practices to boost the overall level of cybersecurity in the EU including measures to ensure (i) Member States' preparedness to tackle cyber-risks, by requiring them to be appropriately equipped, for example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority; (ii) cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States; and (iii) a culture of security across sectors that are vital for the EU economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Moreover, improving cybersecurity is an objective that is pursued in several other European on-going initiatives including the European strategy for data, which promotes an effective use of data in the EU and the report of the European Parliament on digital finance, which inter alia calls for a common approach on cyber-resilience of the financial sector.
3. The TIBER-EU European framework for Threat Intelligence-Based Ethical Red-teaming established by the ECB is the first EU-wide guide on how authorities, entities and threat intelligence and red-team providers should work together to test and improve the cyber resilience of entities by carrying out a controlled cyberattack. It constitutes a European framework for putting in place voluntary programmes to test and improve the resilience of financial infrastructures and institutions against sophisticated cyber-attacks.
4. For example the BCBS consulted on principles for operational resilience in the banking sector in October 2020.
5. Domestic requirements include reporting obligations of operational events to domestic supervisory authorities and threat-led penetration testing frameworks. Threat penetration testing is also mandatory at the EU level for certain types of financial market infrastructures (FMIs).

Following a public consultation conducted by the Commission on the DORA legislative proposal, which ended in May 2021, negotiations involving the European Parliament and the Council have started. The aim is to have the regulations in the Digital Finance package, including DORA, in full effect by 2024.

2. ICT risk management measures

DORA proposes a harmonised approach to ICT risk management across financial services sectors, covering three main elements: ICT risk identification and mitigation, ICT incident reporting and information sharing and digital operational resilience testing. While the proposed set of rules will apply to all financial sector players, requirements are planned to be enforced proportionally in order to be tailored to a firm's size and business profile.

Market stakeholders generally support the streamlining of ICT risk management and reporting at EU level proposed by DORA, which should reduce inefficiencies and legal uncertainty for market players due to the current differing and overlapping requirements and also facilitate the supervision of ICT risks, thus contributing to enhance operational resilience at overall market level. Some market players have emphasized the importance of a proportionate approach to these requirements and also stressed that the common framework defined by DORA should remain flexible enough to manage future evolutions and risks.

2.1 ICT risk identification and mitigation

Under DORA, financial entities would be required to create and maintain a solid and comprehensive ICT risk management framework allowing the identification, classification and documentation of ICT risks. This must include a dedicated and comprehensive business continuity policy, disaster recovery plans and a communication policy to customers and stakeholders. Alongside this framework, financial entities would have to follow certain requirements for the use and maintenance of ICT systems, identify and analyse risks on a continuous basis, design and implement security and threat-prevention measures and promptly detect anomalous activities. These measures need to be approved and overseen by the management of financial entities who will bear the final responsibility for managing ICT risks.

2.2 ICT incident reporting and information sharing

Financial entities would need to establish and implement a robust ICT-related incident reporting process and to put in place early warning indicators. This involves classifying ICT-related incidents, according to prescribed criteria to be established at EU level and reporting all "major" ICT-related incidents and their potential root causes to their national competent authority (NCA) within predetermined timeframes[6]. DORA also proposes the establishment, at a later stage, of a single EU hub for ICT-incident reporting in order to streamline incident gathering at the EU level, replacing the current reporting to domestic NCAs. Moreover, concerning interconnected ecosystems, DORA would allow the exchange of information and intelligence on ICT risks and cyber-threats between financial entities in order to enhance risk prevention and mitigation.

2.3 Digital operational resilience testing

Financial entities would need to test their ICT risk management frameworks on a regular basis, so that they can prove their readiness to handle any potential disruption from ICT use and also demonstrate that they are in a position to identify and solve possible failures. Common standards for digital operational resilience testing[7] are due to be defined in a proportionate way to the size, business and risk profile of financial entities. A mutual recognition of tests across EU Member States is also foreseen, in order to ensure that firms do not face duplicate requirements in the EU and that supervisors can optimize their resources.

At the end of the tests carried out at least every 3 years, financial entities would be required to communicate the agreed reports and remediation plans to the competent authorities and confirm that penetration tests have been performed in accordance with the requirements. These requirements and the application of mandatory threshold criteria are likely to increase the number of entities conducting threat penetration testing, and the cross-border recognition of tests should also help to reduce duplications across Member States for cross-border firms.

3. Management of ICT third-party risks

The second main pillar of the DORA proposal concerns the management of ICT third-party risks by financial entities.

First, and building on the ESA's cloud outsourcing guidelines, DORA proposes principles-based rules for the monitoring by financial entities of risks arising from the use of ICT third-party providers and the harmonisation of key elements of the relationship between financial entities and ICT third-party providers. This includes standard terms and clauses for the establishment of outsourcing contracts, notably

6. Three types of reporting to the NCAs have been identified: (i) initial notification no later than the end of the business day; (ii) intermediate report no later than one week after the initial notification, providing a status update; (iii) final report when the root cause analysis has been completed, no later than one month after the initial report, regardless of whether or not mitigation measures have already been implemented.

7. Beyond the testing of ICT tools, systems and processes based on threat led penetration testing this involves a range of tests including vulnerability assessments and scans, open source analyses, network security assessments, penetration testing and source code reviews, when feasible. The technical standards to apply for conducting intelligence-based penetration testing are due to be developed by the joint ESAs and are likely to be aligned with the voluntary TIBER-EU framework developed by the ECB.

for cloud computing services, the identification of circumstances in which such contracts must be terminated and the granting of auditing rights for financial entities outsourcing these services.

Secondly, DORA seeks to improve the management of risks posed by ICT third-party service providers that may be considered to be 'critical' for the functioning of the financial sector, by subjecting them to an EU level oversight framework. As per the Commission's proposal, this framework involves first the designation by the ESAs Joint Committee of critical ICT third-party service providers (CTPPs) based on criteria such as the systemic impact of a potential failure of the provider, the systemic character of financial entities that rely on the service provider and its geographical coverage and degree of substitutability. For each of the CTPPs identified, one of the ESAs would be appointed as Lead Overseer[8] in charge of monitoring at the EU level the rules, procedures and mechanisms put in place by the CTPP and evaluating whether they are sufficient to manage the risks that it may pose to financial entities. In terms of powers, the Lead Overseer would have an unrestricted right to access all information that is necessary to carry out its duties, including all relevant business and operational documents, contracts and policies. Powers would also be granted to the Lead Overseer to conduct on-site inspections of any premises of CTPPs and possibly impose fines if CTPPs fail to comply with requirements. Finally the DORA proposal also includes rules concerning third-country ICT providers, preventing EU financial firms from using the services of an ICT third-party provider that is 'established' in a third-country and that would be designated as 'critical' if it was established in the EU[9].

The recommendations concerning the oversight of CTPPs have raised a number of comments and questions from supervisors and market stakeholders. In a letter sent in February 2021 to the European Commission, Parliament and Council, the chairs of the ESAs were supportive of these recommendations but they emphasized the need to grant the ESAs with the appropriate powers and mandate, along with the necessary resources and expertise, for conducting this oversight. They also highlighted a certain number of areas that need clarifying, including the way the oversight of a CTPP providing ICT services to the entire financial sector should be conducted and the scope of services this oversight should cover. Regarding this latter point, some market participants have suggested limiting the oversight scope to the services of CTPPs used for critical or important functions of financial entities. Issues raised by some market players also concern the restrictions on the use of third-country service providers proposed in DORA. Certain players argue that this measure may lead to greater concentration risk and reduced choice for financial players, ultimately impacting their competitiveness. Clarifications are also asked about the service providers that this rule may apply to and notably whether intra-group ICT providers would be concerned. The fact that the criteria for determining CTPPs should be based on the materiality and impact of the outsourced services, rather than on the type or scale of the ICT provider, was also stressed by certain market participants.

Concerning the monitoring of ICT third-party risks by financial entities, some financial market players have asked for further assurances for being in a position to implement audit and inspection requirements concerning large ICT service providers and emphasized that the termination of a contractual relation with a CTPP in particular should only be used as a last resort solution, given the potential operational challenges and possible impacts on financial stability. The interactions between DORA and the NIS2 Directive are a further issue to be tackled particularly for CTPPs[10]. While DORA should generally prevail over the NIS Directive for financial entities, the fact that non-financial third-party ICT providers would be subject to overlapping and possibly inconsistent or conflicting rules due to inconsistencies between DORA, NIS2 and the ESA cloud outsourcing rules has been emphasized requiring a further harmonisation of these frameworks in the context of the on-going legislative process[11]. The need to ensure that these frameworks remain fit-for-purpose and consistent in the future with continuously evolving technologies has also been stressed.

8. The Joint Committee and the ESAs would be supported in this task by an Oversight Forum carrying out preparatory work for the decisions and recommendations concerning CTPPs.

9. In preamble 58 to the Commission's DORA proposal it is mentioned that this requirement for legal incorporation in the Union of ICT third-party service providers which have been designated as critical does not amount to data localisation since DORA does not entail any further requirement on data storage or processing to be undertaken in the Union.

10. This issue has been mentioned for example by the ECB in its Opinion on the DORA proposal (4 June 2021). See also Eurofi April 2021 Seminar Summary 'EU financial data space and cloud infrastructure: is the EU moving in the right direction?'.

11. Article 29 (5) of the Commission's DORA proposal states that the CTPP oversight requirements are without prejudice to the application of the NIS Directive and of other Union rules on oversight applicable to cloud computing services, therefore there is a risk of overlap. Whether there will be conflicting or inconsistent rules depends on how the Lead Overseer and the NIS2 competent authorities will fulfil their roles.