Whitepaper

Digital Operational Resilience Act:

The enhancement of digital resilience in EU's financial sector

CGI

Introduction

Over the past couple of years, the European Commission has developed a number of advancing legislative proposals, aiming for “a Europe fit for the digital age” as Commission President Ursula von der Leyen reveals the project[1]. With proposals such as the *Digital Services Act*[2] and the *Digital Markets Act*[3] gaining most international attention, less noticed proposals slip through to only specialist and sectorial circles.

In September 2020 the European Commission issued a completely new regulatory framework, the draft for the **Digital Operational Resilience Act** (DORA) as part of the *Digital Finance Package* (DFP)[4]. The proposal largely builds on already existing regulatory requirements introduced by various European regulators, and combines these into one regulation. The DORA reforms, so to say, existing EU sectoral regulations in light of the developments in digital technology and changes in the sector caused by this. Before the proposal is employed, there is no objective ICT risk management standard as a unified approach in Europe.

The DORA aims to establish a much clearer foundation and shifts the focus from ensuring firms’ financial resilience, to also ensuring they can maintain resilient operations through an incident of severe operational disruption – such as during a cyberattack.

The urgency for such a proposal comes from the deep concerns expressed by the *European Systemic Risk Board*[5], who advised the need to unify and strengthen the third-party risk management requirements in financial entities across Europe. This recommendation followed a report on cyber incidents in the financial sector, identifying cyber risk as being one of the greatest risks and recognizing that one single event could potentially trigger a systemic crisis, threatening financial stability across Europe. As financial firms rely more and more on their digital systems, the EU decided to urge firms in ensuring operations to be as resilient as possible.

This sense of urgency and the increasing need for better resilience follows the recent increase of cyberattacks, with Europe's financial sector as a repeated target for these intrusions. While cyberattacks cannot simply be avoided altogether, financial stability in Europe – and therefore the impact on the global financial sector – can still be achieved if organizations mitigate the repercussions of cyber threats on ICT.

The increase in cyberattacks was also perceived during the COVID-19 pandemic, where the importance of *remote access* for financial services greatly increased, and with that the use and reliance on ICT of the financial sector. The European Commission stated that cyberattacks on financial institutions has risen by 38% since the pandemic began, without a uniform manner on safeguarding[6]. This calls the need for a better regulation, to ensure the withstanding of financial entities during potential ICT disruptions and thus addressing cyber incidents and threats.

Global scope

DORA creates a single, unified framework for regulating risk management for financial entities operating in Europe, and mandates a common approach to cybersecurity for ICT across all 30 countries in the European Economic Area[7].

Its authority will be felt worldwide, as it will have substantial impact on how any ICT provider or large financial organization does business in Europe, and how financial entities use software-as-a-service technology over its life cycle. The regulation affects any ICT provider of financial services, financial technology businesses and businesses designated as critical vendors operating in Europe, regardless of whether those vendors are based in Europe or anywhere else in the world. All are required to be compliant with DORA's requirements, or else face substantial penalties as the *European Supervisory Authorities* (ESA's) will be authorized to access critical ICT third-party service providers directly – and sanction them if necessary.

However, there are restrictions designed in the proposal to who may do businesses with EU's financial entities. Although DORA would not directly restrict cross-border data transfers between these entities and third-party ICT providers, several of the stated provisions could lead to that consequence. The use of non-EU providers and their services could be indirectly limited if they are supplied from outside the EU. One of the provisions (Article 26.2[8]) would impose special obligations for entities that allow their EU-based ICT provider to sub-contract critical or important functions to a provider in a non-EU based country. Technically, ICT-subcontractor's foreign status is disqualifying by definition. Nonetheless, the provision does appear to establish the presumption that the choice of a non-EU based contractor would be a complicating factor for an EU-based financial entity.

This builds on the next provision, where it is stated that financial entities may not utilize companies without business presence in the EU for their critical ICT services. Although there is no textual reason stated for this restriction, it may be presumed that the Commission considers the third-party's business presence in an EU member state to be legally sufficient as a basis for exercising jurisdiction and demanding data, if deemed necessary. It is also stressed that this particular provision is not a data localization requirement – *"the regulation does not entail any further requirement on data storage or processing to be undertaken within the Union"* as DORA Article 28.9 quotes[9].

As this may be speculated to be for competitive reasons, the proposed DORA legislation needs to better the articulation on how the proposed limitations on third-party services located outside of the territorial scope comport with non-discrimination obligations in trade law or may be justified by relevant exceptions.

As one of the main reasons behind the regulation is to harmonize rules on ICT risk management, DORA's scope of application is certainly broad. It covers all financial actors within the EU from credit institutions to AIFMS, payment institutions, insurance companies and

statutory auditors. The requirements are also based on proportionality: while the rules cover all financial entities, their applicability will depend on numerous variables, such as size, activity and the overall risk it is subject to. The applicability extends to 20 types of regulated EU financial entities, such as banks, stock exchanges and clearinghouses, as well as fintechs. Outside of DORA's reach remain payment systems and card payments schemes.

In order to set the bar at a level which doesn't compromise new entrants to the financial markets, a 'sliding scale' of thresholds of application makes sure that the larger the risk from the operation (or the more critical the service to the financial markets), the more stringent the application of the law is.

Noteworthy is to pay attention to the United Kingdom government hinting that it will legislate for a UK-equivalent of the EU's DORA. These plans have been foreshadowed in Her Majesty's Treasury, outlining a proposal to also regulate third parties to financial services and financial market infrastructure firms. Similarly to DORA, the UK proposal also aims to allow regulators to directly oversee the services provided by critical third parties and aims for a heightened resilience.

Similarities and Continuation

As DORA builds upon existing regulations, the EU states that the regulatory complexity will be reduced, together with lowering the financial and administrative burdens caused by the current patchwork of regulations.

The proposal represents the first attempt to streamline and harmonize EU-level requirements for the ICT risk management. In the past we have seen minimum intervention of the EU in the field of cybersecurity, with overly general rules that lead to own interpretation by national authorities. In contrast to other EU legislation in the field of cybersecurity, most notably the *General Data Protection Regulation* (GDPR) and the *Network and Information Systems Directive* (NIS), DORA is not a principle-based piece of legislation and instead contains detailed lists of requirements to boost the operational and security capabilities of affected businesses.

Where the DORA differs from the NIS/NIS2, is what sectors both are applicable to. NIS applies to most businesses and sectors, while DORA applies to only the financial sector and their critical third-party ICT providers. The possible overlaps between the two are addressed via a *lex specialis* exemption, meaning that in case of conflict, DORA applies first.

A similar set of rules are found in the *Cyber Security Framework* (CSF) as advisory recommendations, published by the *National Institute of Standards and Technology* (NIST). The contrast between these two is that while CSF guidelines are purely advisory, DORA commands compliance and requires demonstration of meeting the conditions stated in the regulation.

Authorities

For supervising the affected financial entities and associated *Critical Third-Party Providers* (CTPPs) to ensure compliance to the regulatory standards, one of the three *European Supervisory Authorities* (ESAs) will be appointed:

- The European Banking Authority (EBA)[10]
- The European Insurance and Occupational Pensions Authority (EIOPA)[11]
- The European Securities and Markets Authority (ESMA)[12]

One of the three will be appointed as *'Lead Overseer'* for each CTPP. The appointment of each ESA to a CTPP is chosen based on the total value of assets of the financial entities using the CTPP's services. The monitoring of CTPP's is used to avoid a so-called domino effect, where the heavily interconnected financial sector could fall due to one single trigger event.

Five pillars of DORA

Once the new regulation comes into force in late 2022 with an expected two-year transition period, EU financial firms will be expected to comply with the newly stated requirements in the following five pillars of the DORA:

Digital Operational Resilience Testing

- Obligation to implement a proportional and risk-based digital operational resilience testing program for a full range of appropriate tests,
- Test ICT risk management frameworks on a regular basis,
- Ensure the prompt implementation of correct measures,
- Critical ICT systems and applications must be tested annually.

To make sure that the reliability of the ICT defenses is established, financial entities should undergo regular digital operational resilience testing, conducted by either internal or external parties. The regular testing consists of a digital resistance testing program, involving the testing methodologies, testing procedures and tools, the frequency of resilience tests and the prioritization strategy for testing policies.

This pillar could sound familiar to the financial sector, as Threat-Led Penetration Testing frameworks are currently mandatory for certain Financial Market Infrastructures. The DORA will expand testing requirements across the whole financial services sector, increasing the number of entities required to conduct mandatory testing. The proposal assumes a yearly test for all critical ICT for every financial entity at the very least.

The proportionate application of the DORA proposal is most evident in this pillar, as basic testing is obligatory for all financial entities, and advanced testing is only required for financial entities identified as significant by the competent authority. This is based on criteria outlined in the regulation and further developed by the ESAs.

ICT Risk Management

- Comprehensive ICT risk management framework guiding all relating to ICT risk management,
- Streamline and upgrade existing rules on ICT governance,
- Explicit obligation on management to develop and maintain their knowledge of ICT risk,
- Financial entities are required to implement an internationally recognized information security management system.

The ICT risk management requirement a set of key principles revolving around specific functions (e.g. identification, protection and prevention, detection, response and recovery, learning and evolving, communication). These security themes can be traced back to the current technical standards and industry's best practices. The entities that fall under DORA need to identify on a regular and continuous basis what all sources of their ICT risk set-up are, to put protection and prevention measures in place, to promptly detect abnormal and suspicious activities, and to set up dedicated and comprehensive business continuity policies, next to disaster and recovery plans.

The final responsibility for managing ICT risk is left for the management body of the financial entity. The DORA sets out a list of duties and obligations to which management is subject, such as the explicit obligation to develop and maintain their knowledge of ICT risk. Furthermore, financial entities are required to identify their ICT risk landscape and have a comprehensive and extensive ICT risk management framework in place, guiding and steering all work relating to ICT risk management.

ICT Incident Reporting

- Implement ICT-related incident management process and develop capabilities to monitor, handle and follow-up on incidents,
- Submit initial, intermediate and final reports on ICT-related incidents to relevant competent authority, in line with process set out in the proposal,
- Incidents classification according to factors outlined in the proposal, e.g. geographical spread, affected services' criticality and incident duration.

DORA also states the reporting obligation to entities, next to the establishment and implementation of a management process, meant to monitor and log ICT-related incidents. These incidents will then be classified based on criteria documented in the proposal and developed by the ESAs. When the incident is classified as major, it must be reported to the relevant competent authority and formatted in a common template to ensure the procedure to be as harmonized as the ESA's intent it to be. In the instance of an incident happening, financial entities must submit initial, intermediate and final reports. Next to that, clients and users should be informed where the incident has or may have an impact on their financial interests.

Furthermore, DORA will create a more streamlined reporting channel for ICT-related incidents, which is a welcomed improvement of the current multiple reporting requirements. Reporting trigger events should be reduced and the format for reporting will be harmonized. This completely streamlined reporting channel leads to a single EU-hub, instead of multiple *National Competent Authorities* (NCAs).

This EU-hub will collect all reports of major ICT-incidents impacting financial entities, whereby the gathered data will reveal common vulnerabilities and trends across the financial sector. According to the new EU reporting rules, all financial firms will need to submit a root cause report within one month of a major ICT-incident. To support the timely submission of such reports, financial entities will need to implement reliable early warning indicators of ICT disruptions.

Information & Intelligence Sharing

- Raise awareness of new cyber threats, reliable data protection solutions and operational resilience tactics,
- Sharing within trusted communities and is carried out in accordance with applicable legislation (e.g. data protection, trade secrets and competition).

In addition to the reporting requirements, the proposal also stresses the function of learning and evolving in information sharing and exchanging cyber threat information between entities within trusted financial communities. The objective of such information-sharing is to raise awareness of new cyber threats, reliable data protection solutions and operational resilience tactics.

ICT Third-party Risks

- Establish framework for critical ICT third-party risks,
- Adopt and regularly review a strategy on ICT third-party risk,
- Maintain a register of information, control outsourcing contracts and arrangements,
- Perform ICT concentration risk assessments before entering into new contractual arrangements.

One of the most noteworthy aspects of DORA is its focus on third-party risk. Even though the financial sector relies more and more on ICT firms, there seems to be a lack of specific powers to address ICT risks arising from those third parties. The act would put critical third-party service providers into the scope of regulators and subject them to an oversight framework at EU-level.

This is probably the most challenging pillar of the DORA. Providers, such as Cloud Services, will be forced to comply with regulators if they are classified as *'critical'*. Some of the factors that would classify a third-party service provider as critical include:

- *Degree of substitutability* – CTPPs are more difficult to replace in the event of an operational disruption (either occurring internally or in the vendor's environment)
- The *number* of financial entities relying on the CTPPs for operational continuity

Once designated as critical, oversight of the third-party will be carried out by one of the ESA's, who will be able to conduct inspections on-site and off-site, issue recommendations and levy fines of up to 1% of the daily worldwide turnover, on a daily basis for the maximum period of 6 months in case of non-compliance[13].

How can we help?

Although DORA is still only a proposal, financial entities are advised to start working towards compliancy with the stated requirements.

DORA is a much welcomed catalyzer for the efforts to build the digital single market for financial services, as current circumstances call for the introduction of a harmonized framework at EU-level. While some obligations are not expected to pose major changes and impact to current ways of working and standing frameworks, others may require more effort and time. As the DORA moves towards finalization, firms need to be mindful of the scale of the challenge that implementation will bring. A two-year implementation period will be a short window of time to get things right. Therefore businesses simply cannot afford to wait for the political process to conclude, and should already be considering what successful implementation requires from them.

Bearing in mind that it can be a time-consuming matter to familiarize ourselves with these requirements - on both legal and technical level - and to ensure compliancy, the developments following this proposal should not escape your attention. Our professionals can help you to understand the new obligations and support you through the transformation. Understanding the requirements and recognizing the gaps is key to optimal developments and growth. See our dedicated services to help you comply with all necessary regulations and make sure you are fully prepared of what is to come.

References:

1. A Europe fit for the digital age
2. The Digital Services Act: ensuring a safe and accountable online environment
3. The Digital Markets Act: ensuring fair and open digital markets
4. Digital finance package
5. Systemic cyber risk
6. A digital finance strategy for Europe
7. EUR-Lex - 52020PC0595 - EN - EUR-Lex
8. EUR-Lex - 52020PC0595 - EN - EUR-Lex
9. EUR-Lex - 52020PC0595 - EN - EUR-Lex
10. The European Banking Authority
11. The European Insurance and Occupational Pensions Authority
12. The European Securities and Markets Authority
13. EUR-Lex - 52020PC0595 - EN - EUR-Lex

About CGI

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

cgi.com