DIGITAL OPERATIONAL AND CYBER-RESILIENCE

STEVEN MAIJOOR
Executive Director of Supervision - De Nederlandsche Bank (DNB)

DORA: catching up to new realities and risks in the financial sector

In the years following the 2008-09 financial crisis, financial regulators were - understandably – focused on mitigating financial risks. However, as financial services have become increasingly digitalized, and as the digital transformation of the financial sector is set to continue to gather pace, it has become clear that the regulatory framework for ICT risks and digital operational resilience is in need of an update; and indeed of an upgrade. The DORA political agreement provides this by laying down a comprehensive framework for digital operational resilience.

The challenge for policymakers and supervisors now is to shape the implementation of DORA in a way that enables effective and efficient supervision and oversight, ensures proportionality, maintains alignment with other relevant legislation (e.g. NIS2 and CERD), and is focused on delivering on the ultimate objective of DORA: safeguarding business resilience; the resilience of financial (business) services – especially important and critical ones – provided by financial entities to the wider economy.

Realizing this ultimate DORA objective first of all requires that – as part of the DORA implementing legislation – a holistic implementation framework for managing ICT- and third-party risk is set up. Such a framework should start from the identification of individual services provided to external users by financial entities; and of the resources used in delivering them, including ICT infrastructure and third parties. Next, resilience requirements can be set for each service, based on its importance. Stress-testing the resources chain can then inform specific requirements for both the ICT infrastructure and third parties involved in the delivery of the service. Such requirements include strategies for disaster recovery, redundancy requirements, and contract terms with third-party providers.

The DORA implementation framework should be geared towards ensuring business resilience.

Creating a framework focused on the resilience of the delivery of important financial services would prevent ICT- and third-party risk management requirements from becoming tick-the-box exercises, and allow for the integration of ICT risk management into the overall Enterprise Risk Management framework. Moreover, such a framework would inherently enable a proportionate and risk-based implementation of DORA, as differentiation would be based on the importance of the ultimate service provided. Finally, it would enable effective, efficient and convergent implementation of DORA across the EU.

In addition to the overall structure and focus of the DORA implementing legislation, policymakers should also pay particular attention to what will arguably be the most impactful new elements of DORA: the drafting of a Threat-Led Penetration Testing (TLPT) standard, and the implementation of oversight of critical third-party providers (CTPPs).

The TIBER-EU (Threat Intelligence Based Ethical Red teaming) framework is a TLPT framework for financial entities that are critical for financial stability in the EU. It has already been adopted by a large number (17) of central banks, including the ECB. Given both the quality of the TIBER-EU framework and its high take up, it would be most effective and efficient for the new TLPT standard - to be drafted as part of DORA implementation - to follow the TIBER-EU framework. At the same time, the new standard can incorporate differentiation: it can include proportionate requirements for less critical entities, while going beyond the current TIBER-EU framework for the most advanced and critical financial entities and their CTPPs.

CTPPs will not only play a role in TLPT testing; DORA also enables direct oversight of CTPPs by financial supervisors. While key to ensuring the fragmenting financial-services chain can be adequately supervised, this direct oversight will also impose substantial responsibilities on financial supervisors; in particular the European Supervisory Authorities (ESAs), who will serve as Lead Overseers. Cooperation amongst the ESAs - and between ESAs and national supervisors - will be vital to ensuring effective oversight.

Some CTPPs, however, are critical not just to the financial sector, but for the broader economy. This is in particular the case for cloud providers, which will also be regulated nationally under the revised NIS Directive. Therefore, over the medium term, consideration should be given to creating an EU-level, cross-sectoral cloud supervisor. Such a supervisor should be responsible for supervising the stability of major cloud providers, and its board could consist of a number of relevant EU-level supervisors - including European financial supervisory authorities – jointly supervising cloud providers.

In summary, DORA represents a key step in enabling regulators to catch up with the new realities and risks in the financial sector. It is now for policymakers and supervisors to work on implementing legislation and an oversight framework that are effective, proportionate and holistically focused on the resilience of financial services.

EMMANUEL ROCHER

Director for International Affairs - Autorité de Contrôle Prudentiel et de Résolution (ACPR)

DORA: implementing an innovative horizontal supervisory framework for ICT risks

Since the 1970s and 1980s, finance has been a major user of Information and Communications Technology (ICT), digitalising large areas of its businesses and support functions. Not surprisingly, digital risk has long become the first operational risk for banks. As part of their efforts to enhance the resilience of the financial sector facing intensified ICT risks, the European co-legislators reached a political agreement on the Digital Operational Resilience Act (DORA) in May 2022, paving the way for its swift adoption. DORA is not only a major legislative development towards more resilience but it also innovates by reflecting that ICT risks affect all financial entities alike and shall be subject to a common ICT risk management framework. DORA introduces a new set of standards to manage ICT risks for the whole financial sector, in a way that is harmonised at the EU level, enabling to reduce regulatory costs.

The financial sector's resilience to ICT risks had so far been addressed through a fragmented approach consisting of a mix of binding and non-binding standards with significant variations across sectors and jurisdictions. Among them, the Directive on network and Information System security (NIS) covered several key economic sectors but was limited, as regards the financial sector, to banks and market infrastructures. DORA will address ICT risks faced by financial entities horizontally, outside of NIS but in coordination with the revised NIS. As most of the risk management rules set in DORA are already implemented as law, guidelines or best practices, we expect that major financial entities will only have to adjust – not recast – their practices by 2025, when it comes into force.

Beyond ICT risk management, DORA introduces new requirements, whose effective implementation is essential for a proper supervision of ICT risks. DORA will strengthen incident reporting, ICT systems testing and registering third-party providers. Some financial entities are already accustomed to these practices, especially those operating under the payment services directive. For others, these requirements come as an innovation: the implementing acts should duly reflect these diverse situations in setting out requirements whose magnitude and frequency should be proportionate to the risks. Nevertheless, there is a broad consensus that the basic elements of DORA for managing ICT risks and coordinating the response to ICT events should be valid for all financial entities since risks are similar.

A collaborative and agile functioning of the framework will be key to monitor evolving risks.

Introducing an oversight framework for critical third-party ICT service providers (CTPPs) is obviously the most innovative aspect of DORA. This was necessary given the potentially extensive impact of a technical failure on numerous financial entities. CTPPs designated as critical by the Joint Committee of the European Supervisory Authorities (ESAs) will have to hold a legal entity in the EU. All the relevant European and national agencies will join their forces to ensure a proper monitoring of the framework: the oversight tasks conducted by Joint Examination Teams under the lead of one of the ESAs will ensure that CTPPs do not build up exaggerated third-party risks for the financial system. Supervisors will have a better view of the third-party risks and will be able to monitor the effects of concentration or further outsourcing.

The systemic dimension of ICT risks is certainly a focal point for further work. DORA follows a microprudential perspective, but ICT risks can have systemic consequences or be related to system-wide issues. In this regard, DORA allows for an agile coordination between authorities. We welcome the work carried out by the ESRB on the preparedness of European supervisors to tackle financial contagion following an ICT event.

Implementing DORA will be the key challenge going forward. First, it will require significant human and financial resources from the ESAs and the national authorities, especially since ICT skills are constrained and costly to build-up. Secondly, as DORA will imply the intervention of numerous supervisory authorities, we need to build a system that is able to work as a single smart and agile team across Europe. ESAs should also capitalise on the experience of national authorities and the SSM in this matter. It is necessary to prepare for delivering an efficient supervision of ICT risks, in a full and timely manner and with a lean governance.

The first steps, in 2023-2025, will consist for the ESAs in drafting the numerous DORA delegated acts and guidelines. They will define the concrete requirements for financial entities. The implementation of DORA will follow, with the CTPPs oversight becoming effective by 2026.

With DORA, the EU will become a leading jurisdiction in the field of ICT risk management in the financial sector. Its horizontal approach will materialise the essential principle of "same risk – same rule" that ACPR promotes in international fora.

PETRA HIELKEMA

Chairperson - European Insurance and Occupational Pensions Authority (EIOPA)

Digital Operational Resilience: a challenge for the supervisory community

Digital operational resilience refers to the ability of a financial entity to build, assure and review its operational integrity and reliability.

The financial sector has always relied heavily on information and communication technology (ICT) and this reliance grew during the COVID-19 pandemic as customers increasingly used digital services. The dependency on ICT makes financial entities particularly vulnerable to cyber-attacks or incidents, a risk that has become more apparent in the light of Russia's invasion of Ukraine.

The consequences of an attack or disruption of an important cross-border financial service can have far-reaching effects on other companies, sub-sectors, or even the rest of the economy, underlining the importance of digital operational resilience of the financial sector. This makes the policy of European Union's Digital Operational Resilience Act, or DORA, even more relevant.

The current regulatory frameworks cover the ICT risk management and ICT security within the system of governance rules, which have been further detailed by the European Supervisory Authorities (ESAs) and national supervisory authorities into guidelines. For example, the European Insurance and Occupational Pensions Authority (EIOPA) published in 2020 its guidelines on ICT security and governance and outsourcing to cloud service providers.

As such the existing EU legal framework for ICT risks and operational resilience in the financial sector is fragmented, with differences by type of financial entities and by Member State.

For example, although the European Central Bank's work in developing TIBER EU – the European framework for threat intelligence-based ethical red-teaming – has provided some convergence, almost every Member State has its own rules (for example, for carrying out resilience tests) and supervisory approaches (for example, for ICT third-party dependencies) leading to a lack of level playing field, challenges for cross border operating institution and also insufficient consideration of certain ICT risks.

DORA provides a comprehensive set of rules for the supervision of digital operational resilience.

Cross-border financial entities are under increased administrative and financial burden as a result of duplicative requirements and inconsistent provisions, such as the Directive on Security of Networks and Information Systems (NIS Directive) – which does not cover the insurance sector at European level, but has been included in the scope by some Member States – EU legislation on financial services, and national regulations (for example, for reporting incidents).

So the first thing that DORA will bring is harmonisation of the rules relating to operational resilience for the financial sector. As DORA will be lex specialis to the NIS Directive, DORA will cover the following important pillars: ICT risk management; ICT incident reporting; the tests of the operational resilience of ICT systems; and the management of ICT third party risks including an oversight framework of the Pan-European critical ICT service providers (CTPPs).

DORA also will enhance the cooperation among competent authorities including from different sectors (NIS authorities) and jurisdictions in relation to ICT and cyber risk management. It has already enabled the issuance of a European Systemic Risk Board recommendation to the ESAs to set up a pan-European systemic cyber incident coordination framework for relevant authorities.

Finally, DORA will provide for a framework on the basis of which oversight can be implemented on CTPPs, thereby no longer addressing the operational risks via the outsourcing arrangements of the financial institution, but also directly at the CTPP.

There will of course be challenges for supervisors. First there will be the need for the overall integration of DORA supervision into broader supervisory processes. In addition, the speed of technological change means that supervisors will need to keep pace not only with innovation in the market, but also with the skills required to supervise innovation. This in itself could be challenging given the high competition in the market.

Nonetheless, EIOPA is up to the challenge and will work closely with the other ESAs to contribute to the safety and security of Europe's financial systems.

In conclusion, EIOPA considers the arrival of DORA to be both timely and needed. EIOPA looks forward to contributing to fostering an operationally resilient industry, as part of its work to support the supervisory community and the industry to mitigate the risks and seize the opportunities of the digital transformation – including through the implementation of the DORA.

KSENIA DUXFIELD-KARYAKINA

Government Affairs and Public Policy - Google Cloud

Digital Operational Resilience Act: providers preparing for the new framework

DORA is an important framework to harmonize how financial entities must report cybersecurity incidents, test their digital operational resilience, and manage ICT third-party risk across the financial services sector and European Union (EU) member states. In addition to establishing clear expectations for the role of ICT providers, DORA will also allow financial regulators to directly oversee critical ICT providers. Google Cloud welcomes DORA.

As part of our Cloud On Europe's Terms initiative, we are committed to building trust with European governments and enterprises with a cloud that meets their regulatory, digital sovereignty, sustainability, and economic objectives.

We recognize the continuous effort by the European Commission, European Council, and European Parliament to design a proportionate, effective, and future-proof regulation. We have been engaging with the policymakers on the DORA proposal since it was tabled in September 2020, and appreciate the constructive dialogue that the legislators have held with ICT organizations. We firmly believe that DORA will be crucial to the acceleration of digital innovation in the European financial services sector.

Here are a few key benefits of DORA:

- **Coordinated ICT incident reporting:** DORA consolidates financial sector incident reporting requirements under a single streamlined framework. This means financial entities operating in multiple sectors or EU member states should no longer need to navigate parallel, overlapping reporting regimes.
- **New framework for digital operational resilience testing:** Drawing on existing EU initiatives like TIBER-EU, DORA establishes a new EU-wide approach to testing digital operational resilience, including threat-led penetration testing. By clarifying testing methodology and introducing mutual recognition of testing results, DORA will help financial entities continue to build and scale their testing capabilities in a way that works throughout the EU. Importantly, DORA addresses the role of the ICT provider in testing and permits pooled testing to manage the impact of testing on multi-tenant services like public clouds.

At Google Cloud, we share the objectives of DORA and preparing our compliance readiness programs.

- **CoordinatedICT third party risk management:** DORA builds on the strong foundation established by the European Supervisory Authorities' respective outsourcing guidelines by further coordinating ICT third-party risk management requirements across sectors, including the requirements for contracts with ICT providers.
- **Direct oversight of critical ICT providers:** DORA will allow financial regulators to directly oversee critical ICT providers. This mechanism will create a direct communication channel between regulators and designated ICT providers via annual engagements, including oversight plans, inspections, and recommendations. We're confident that this structured dialogue will help to improve risk management and resilience across the sector.

How Google Cloud is preparing for DORA

While DORA isn't expected to take effect until 2024 at the earliest, here's four important topics that DORA will impact and what Google Cloud does to support our customers in these areas today.

- **Incident reporting:** Google Cloud runs an industry-leading information security operation that combines stringent processes, a world-class team, and multi-layered information security and privacy infrastructure. Our data incident response whitepaper outlines Google Cloud's approach to managing and responding to data incidents. We also provide sophisticated tools and solutions that customers can use to independently monitor the security of their data, such as the Security Command Center.
- **Digital operational resilience testing:** We recognize that operational resilience is a key focus for the financial sector. Our research paper on strengthening operational resilience in financial services by migrating to Google Cloud discusses the role that a well-executed migration to Google Cloud can play in strengthening resilience. We also recognize that resilience must be tested. Google Cloud conducts our own rigorous testing, including penetration testing and disaster recovery testing. We also empower our customers to perform their ownpenetration testing and disaster recovery testing.
- **Third-party risk:** Google Cloud's contracts for financial entities in the EU address the contractual requirements in the EBA outsourcing guidelines, the EIOPA cloud outsourcing guidelines, the ESMA cloud outsourcing guidelines, and other member state requirements. We are paying close attention to how these requirements will evolve under DORA.
- **Oversight**: Google Cloud is committed to enabling regulators to effectively supervise a financial entity's use of our services. We grant information, audit and access rights to financial entities, their regulators and their appointees, and support our customers when they or their regulators choose to exercise those rights. We would approach a relationship with a lead overseer with the same commitment to ongoing transparency, collaboration, and assurance.

STEPHEN HESTER

Vice Chair of the Board and Board Member - Nordea Group

Digital operational resilience requires European solutions

Digital operational and cyber resilience has undoubtedly never been subject to such focus as it is currently. Following the pandemic, working models throughout banks' value chains are being digitised at a faster pace than ever before. At the same time the war in Ukraine has raised geopolitical tensions to a new level in Europe, with strong concerns about the impact on cyber security in society and the economy. Although these events could not have been foreseen they underscore the importance of EU's Digital Operational Resilience Act (DORA), as part of the EU's Digital Strategy launched in 2020.

Nordea has welcomed the DORA initiative, in particular as a means to ensure a harmonised framework for delivering operational resilience within the financial services sector in the European single market. A harmonised framework, alongside a speedy delivery of Level 2 requirements, providing clear standards for implementation, will be crucial in ensuring a successful implementation and in turn to avoid fragmentation of the single market.

Opportunities

DORA clearly presents opportunities for the financial sector. It supports a journey towards increased resilience, a journey many banks are already on. Digital resilience is one key aspect, but banks in Europe, Nordea included, are already assessing resilience across several areas: resilience in portfolios, climate issues, and people management for example.

A challenge, or call to action rather, to us as an industry is to see the business case in DORA and other related regulations. This is not just about closing a compliance gap, but to consider our overall strategies and our journey towards a resilient banking sector in Europe. A sector which is fit to support Europe and its companies, entrepreneurs and citizens in the digital age. Nordea is certainly committed to play our part in Europe's digital and sustainable future.

A pan-European framework is needed

As the leading cross-border bank in the Nordic region Nordea considers it crucial that we succeed in creating a common European framework for digital operational and cyber resilience, to ensure that banks and companies can operate smoothly across borders in the single market on equal terms. For Nordea our home market is made up of the four Nordic countries (Denmark, Finland, Norway and Sweden). The opportunity to apply one joint, strong, pan-Nordic approach to digital operational resilience is key to delivering the best service to our customers and the most efficient operational resilience.

It is crucial that we succeed in creating a European framework for digital operational resilience.

National initiatives are to an extent understandable, particularly given the current European security situation. However, we must ensure that such initiatives do not result in overlaps, inconsistencies or duplicative requirements. Any such overlaps would make it more difficult for banks to finance the European economy and provide the critical financial infrastructure needed. As foreseen in the EU's Digital Strategy, fragmenting the single market with national initiatives could even undermine the stability and integrity of the European financial sector, and jeopardise the protection of consumers and investors.

The developments this spring in Europe have certainly shown that joint European action can be strong and effective. However, we need to be even stronger and more united, also in the field of digital and cyber resilience. The aim should be joint action and measures to strengthen the resilience of the whole European financial sector instead of a fragmented approach.

Speedy finalisation of Level 2 requirements is critical

As with any regulation, it is important that the risk mitigation benefits outweigh the cost of measures taken. Nordea welcomes the proposal that EU supervisory authorities should oversee critical service providers and in general any proposal to standardise and streamline processes around third-party providers. Harmonising cross-border reporting is something we are looking forward to, to ease unnecessary burden for cross-border banks. For example, we do today have issues with the "giants" accepting standard contracts, auditing rights etc. EU rules on contract clauses would help evening out the power balance. Also, one audit/inspection from an EU authority rather than all customers asking for access would be easier for the providers to accept.

However, in order for DORA to be successfully implemented by European banks, and for the framework to succeed in tackling the main risks it aims to address, it is important that Level 2 standards are developed and issued as early as possible. Delayed standards risk creating different solutions in banks aiming to become DORA compliant, and then having to redo the implementation work once standards are issued. Another alternative, equally unsatisfactory, is banks putting off large implementation projects while waiting for standards to be issued, and thus delaying the journey towards a more resilient financial sector in Europe.