CYBER AND DIGITAL OPERATIONAL RESILIENCE POLICY PROPOSALS

DOMINIQUE LABOUREIX
Secretary General - Autorité de Contrôle Prudentiel et de Résolution (ACPR)

A much-needed comprehensive cybersecurity framework for the financial sector

Before the Digital Operational Resilience Act (DORA), the European financial regulatory framework regarding information and communication technology (ICT) and third-party/outsourcing risk management was multi-layered, scattered across multiple binding regulations (EMIR, PSD…) and non-binding guidelines of the ESAs, with undue variations across sectors, however exposed to the same risks. DORA, becoming the unique reference regarding digital operational resilience requirements for regulated financial entities, will greatly simplify and improve the framework.

DORA is being designed to set the right balance between two competing objectives: embracing some specificities from the huge diversity of regulated financial entities and promoting harmonization. It will above all address an important shortcoming of the current supervisory architecture of the financial sector: competent authorities and ESAs will have direct oversight of critical ICT services third-party providers. That will provide them with the means to act upon the main ICT providers which play an essential role for the financial sector, and therefore generate systemically operational risks.

However, during the last part of the negotiation process in 2022, it will be essential to avoid any watering down of the ambition of DORA, in particular regarding the ICT risk management requirements and the oversight capabilities of the newly created Oversight Forum. Besides, some provisions will still have to be complemented and clarified in level 2 texts, to enhance DORA's efficiency, in particular regarding the oversight of critical providers. First, on ICT risk management, some relevant requirements in ESAs existing guidelines, not included in DORA, will usefully be taken on board in the foreseen delegated regulations, such as the content of the ICT security policy.

Second, the requirements applying to "fourth-party risk" will need further specification, in particular to determine the conditions to secure subcontracting of critical functions are.

Lastly, there is still some leeway in sketching out properly the new institutional arrangement and the future Oversight Framework of critical third-party ICT services providers, beyond what DORA already provides for. In particular, we need to work out how each participant authority will cooperate within the Forum and what information the joint examination teams will be able to require from critical providers. It is of the utmost importance to provide to the authorities all operational and legal means to act upon critical providers, including non-EU BigTechs.

Once adopted, DORA's success will also depend on how it is implemented and how the cyber systemic risk is addressed.

Indeed, as of today, despite existing rules, supervisors note that financial institutions still have significant efforts to make to improve their operational resilience. For instance, their information systems are not always sufficiently secured, whereas the massive use of remote-working due to the Covid-19 pandemic creates new vulnerabilities in the face of increasingly sophisticated cyber-attacks. In parallel, the Oversight Forum's capacity to function effectively will depend on the involvement of the designated critical providers. Thus, based on the new framework, a strong commitment by all stakeholders will be necessary to ensure that DORA is consistently implemented across the whole financial sector.

DORA's success will depend on how it is implemented and how the cyber systemic risk is addressed.

Finally, the operational resilience of financial institutions at solo level is not the end of the journey, as the systemic dimension of the cyber risk remains a challenge for regulators. On this matter, DORA encourages more cooperation between authorities at the European level. In its recent report, the ESRB identifies the need for the establishment of a pan-European systemic cyber incident coordination framework (EU-SCICF) to mitigate the risk of a coordination failure[1].

Public authorities and financial institutions will need to commit to put in place this improved mechanism, which implies to overcome some legal, practical and political obstacles in the future.

[1] Mitigating systemic cyber risk, ESRB, January 2022

JOSÉ MANUEL CAMPA

Chairperson - European Banking Authority (EBA)

Promoting Digital Operational Resilience across the EU financial sector

As the legislative procedure on the proposed Digital Operational Resilience Act (DORA) is ongoing, the European Banking Authority (EBA), the other relevant authorities and the financial sector are getting ready for the implementation of the new legislation. Assuring digital operational resilience of the financial system is a common goal to be pursued.

DORA is also the first concrete initiative to address the complex issue of the dependencies on critical ICT third-party providers (CTPPs) in the financial sector. The high-degree of interconnectedness across the financial sector in Europe is clearly materialised in the activities of many of these third-party providers. A small number of them seamlessly provide core services across the financial sector (and beyond) and across member states (and globally). The manner to ensure effective oversight to these services poses a challenge to the EU regulatory framework structured along a mix of European and national supervisory authorities and sectorial mandates. If successfully implemented, DORA could provide a pathway to a broader oversight in the future.

The proposed regulatory and oversight framework for CTPPs should come to complement and reinforce the existing framework for operational resilience of supervised entities. This should neither undermine nor diminish the efforts expected by financial entities to further focus on their digital operational resilience.

On the regulatory side, the European Supervisory Authorities (ESAs) are expected to jointly develop a significant number of Technical Standards to further specify the technical implementing details of the legal requirements. During the development of these mandates it would be important to ensure consistency with the existing sectorial guidance to avoid unnecessary burden to the financial sector.

DORA also proposes the establishment of an oversight framework at EU level for ICT CTPPs. The role of the ESAs (as Lead Overseers) is limited to the ICT risks which CTPPs may pose to financial entities. It will neither imply direct supervision of CTPPs in the provision of those services to financial entities nor oversight across their full range of activities. Additionally, the oversight responsibilities will be shared across the three ESAs with one of them acting as the lead supervisor for each CTPP. Therefore, the future structure of this oversight model for CTPPs will need to be carefully crafted to ensure coordination and homogeneity in the oversight. This will require enhanced coordination among the ESAs.

The outcome of the oversight work will inform the micro-prudential supervisory work as the main objective of the oversight work is to strengthen the stability and security of the ICT services provided to financial entities. This will require strong coordination between the Lead Overseers and the supervisors of financial entities as efficiencies should be explored to avoid duplicative, or even inconsistent, tasks. The proposed legal text also empowers such close coordination as supervisors will be able to take measures concerning CTPPs only in agreement with the Lead Overseer. That coordination will need to be made operational. It should be also noted that the proposed oversight framework is not expected to shift in any way the responsibilities of the financial entities to properly manage their ICT third-party risks.

Implementing DORA will demand enhanced coordination among European regulators.

A regular communication between the Lead Overseers and the CTPPs would be envisaged to support the effectiveness of the oversight conduct along with the respective communication between the Lead Overseers and supervisors. Moreover, it will be important to maintain a strong relationship between the financial sector and the other sectors covered by the Network and Information Security Directive (NIS2) for the exchange of information. This could be achieved by participating in the discussions of the NIS Cooperation Group and by exchanging information and cooperating with the single points of contact and with the national CSIRTs under the NIS2 Directive.

MARGARITA DELGADO
Deputy Governor
Banco de España

Regulation and digital operational resilience challenges in Europe

Given the importance of the banking sector in the economy, banks' profits are a fundamental source of capital to support economic growth and preserve financial stability. The low interest rate environment and digital disruption are two of the main challenges currently facing traditional banking. Digital transformation is key to underpinning institutions' profitability, efficiency and new business activities. Moreover, it is necessary to ensure banks remain competitive and can offer their customers personalised services in an agile, efficient and innovative way. But this transformation comes at the price of huge investment and the risks associated with the large-scale use of technological solutions.

The goal of DORA is to mitigate the risks of digital transformation in the EU financial sector by establishing a common framework for enhancing digital operational resilience. It contains provisions for institutions on technology risk management, incident management and reporting, digital resilience testing, third-party risk management and information sharing. Furthermore, to tackle the increasing dependency of the financial sector on third party services, DORA establishes a framework for the direct oversight of those technology service providers that become critical for the EU financial sector as a whole.

All in all, DORA is an ambitious proposal that could be a game changer in making the EU financial sector more operationally resilient. However, it also poses important challenges that need to be addressed.

The scope of DORA is wide, covering institutions of different sizes, business models, risk profiles and complexity. Therefore, when the level 2 regulation is drafted it will be crucial to take into account proportionality, without impairing DORA's goal of establishing a minimum level of resilience even for smaller or simpler institutions. Given the current regulatory fragmentation, some types of institutions will already be compliant with most of the provisions in DORA, while others will need to make a significant effort to comply. Although the text includes some exemptions for smaller institutions, it should be further refined to take into account criteria other than economic size, which is not necessarily directly related to the level of technology risk.

Notably, DORA requires an unprecedented level of coordination and cooperation amongst authorities. Recognising that cyber threats are cross-border and cross-sector, DORA establishes several mechanisms through which authorities will have to exchange information and work together, not only within the financial sector, but also with the cybersecurity authorities in the NIS[1] ecosystem. Establishing clear roles and responsibilities and building trust amongst stakeholders to ensure secure and timely information sharing is, without doubt, another challenge. DORA offers a unique opportunity to build cyber threat intelligence in the EU financial sector, a very powerful tool to enhance its resilience.

As mentioned already, DORA proposes a novel EU framework for the direct oversight of critical technology third parties. This is a completely new set-up with complex governance arrangements, in which it is crucial to ensure that all stakeholders participate effectively and efficiently. In addition, to be able to oversee highly sophisticated technology providers, competent authorities will have to consider whether they have enough resources and technical skills. This is also the case for the European Supervisory Authorities, who have a prominent role to play.

DORA offers a unique opportunity to build cyber threat intelligence in the EU financial sector.

Once in place, the oversight framework will have benefits not only for financial institutions, but also for the affected service providers, by creating a single framework to replace the current fragmented regulatory and supervisory regimes. At the same time, it will allow competent authorities to monitor those providers on which the sector is highly dependent.

To seize the opportunity provided by DORA to enhance the operational resilience of the EU financial sector, financial institutions, third parties and authorities will have to cooperate and work together even more than they do already.

[1] Network and information systems. See Directive (EU) 2016/1148.

JENS OBERMÖLLER

Head of Directorate IT Supervision, Payments, Cyber Security
Federal Financial Supervisory Authority, Germany (BaFin)

DORA - gearing up to become digitally resilient!

In today's financial world, information and communication technology (ICT) is no longer a secondary requirement for generating income, but forms the fundamental infrastructure for nearly all processes and digitalisation and technological innovation in the area of financial services are still gaining pace. This brings many advantages to financial entities but has also made the industry more vulnerable: financial entities, which people entrust with their money and their most private data (including medical data), are among the most popular targets for cyberattacks. Such attacks can cause significant distress to individual companies – and to the market as a whole, even beyond national borders.

Supervisory requirements are one of the most important tools in our arsenal for improving cyber resilience in the financial sector. Due to the highly interconnected nature of this industry, such requirements should apply beyond borders, wherever possible, and should be as consistent as possible throughout the European Union.

By providing sound and effective rules for the management of ICT risks, the DORA legislation establishes a harmonised framework for improving the cyber security of all financial entities at the European level. What is more, as a Level 1 regulation, DORA will send a clear signal that digital operational resilience is just as important as financial resilience.

In Germany, BaFin strongly believes in the benefits of harmonised requirements for the management of ICT risks, and has been following a similar approach since 2016, when it published its Supervisory Requirements for IT in Financial Institutions. This format has since then been replicated for insurers and asset management companies as well as payment service providers – making use of the same terminology and harmonised requirements.

Still – since nowhere in Europe there are as many small and medium sized entities in the financial sector as in Germany – the principle of proportionality is particularly close to our hearts, as German supervisors. While applying the principle of "the same rules for everyone", its proportional approach means that the rules take into account an entity's risk profile. This is essential, particularly in the highly diverse European financial market.

BaFin also greatly appreciates the principle-based foundation of DORA – ensuring technological neutrality and a sufficient degree of flexibility. Still, whatever measures are taken with regard to ICT risks, the fact remains that our efforts to ensure ICT security will never be complete; technology moves far too quickly for that. Something that is considered completely safe today could be a weak point exploited by cyber villains tomorrow. Supervisory requirements need to keep pace with technological change.

Traditionally, the value creation processes at the majority of financial entities took place under one umbrella. Nowadays, an increasing number of processes are performed by third-party service providers. This trend is likely to gain further momentum. Therefore, it is of utmost importance that we, as European supervisors, gain a comprehensive and global view of the outsourcing ecosystem so that we can respond to the potential challenges posed by critical ICT third-party service providers in the financial system. The Oversight Framework established by DORA represents a crucial step forward in tackling these challenges. Given the complex nature of value chains in today's financial sector and the sheer size and global footprint of some ICT service providers, the underlying oversight architecture needs to be carefully designed to ensure that it is both effective and efficient. Moreover, there is a red line that must not be crossed: tasks can be outsourced; responsibility, on the other hand, cannot. It must remain where it belongs: with the financial entities' managers.

Digital operational resilience is an ongoing process: there is no finish line!

Finally, we should not forget that digital operational resilience is an ongoing process: there is no finish line. Even if financial entities met all of these new requirements perfectly, would we ever be able to say our task is complete? Could we ever really claim to be completely resilient? The answer, unfortunately, is probably not.

In an interconnected world, dealing with ICT risks as well ICT third-party risks will always remain a challenge.

JASON HARRELL
Managing Director and Head of External Engagements -
The Depository Trust & Clearing Corporation

EU Digital Operational Resilience: the path to enhanced resilience

Today's financial services industry increasingly leverages technology and ICT providers to extend financial services to excluded or underserved individuals, increase efficiency and lower transactional costs, and diversify financing. To provide greater assurance of a level playing field across Member States and increase the safety and soundness of financial markets, the DORA framework must establish an oversight framework that meets these stated goals. The European Parliament (EP) issued its amendments to the European Commission (EC) text which it will use to enter negotiations with the EC and Council of Ministers. The EP has made significant strides to strengthen the EC's proposal. I believe that this text will ultimately deliver on its expected goals. However, there are areas where further improvements may increase clarity for financial entities.

Operational Resilience Principles

During the DORA negotiations, financial entities and authorities worked to develop operational resilience principles for use by supervisors when developing rulemaking. In 2021, the Basel Committee on Banking Supervision (BCBS) published its Principles For Operational Resilience. These Principles, developed in collaboration with the private sector, defines operational resilience concepts such as critical operations, tolerance for disruption, mapping of interconnections and scenario testing. These activities are to occur at the financial entity's business operations level. DORA has taken these terms and integrated them at the technology level which may lead to financial entities being unclear on their requirements.

As an example, the BCBS Principles require financial entities to map the people, process, technology and suppliers needed to deliver its critical operations while DORA may require that these mappings include technology systems configurations. In addition, DORA requires impact tolerance for ICT disruptions while the BCBS Principles require impact tolerance at the business' critical operation level. Further guidance will clarify financial entities' operational resilience expectations.

Intragroup / Third-Party ICT Relationships

The Proposed Text includes intragroup relationships in the definition of third-party ICT relationships. While intragroup relationships may be external to the covered entity, the parent-to-affiliate relationships deliver numerous common services which may include: IT services, cyber risk, and audit. Further, these relationships provide consistent governance, resource management, and technology alignment that simplify technology service delivery and enhance resilience. The inclusion of intragroup ICT relationships in the definition of ICT third-party relationships by the EP text extends requirements that may not promote stronger resilience.

- *Exit Strategies*
  By changing this definition, financial entities will be required to develop exit strategies for their intragroup ICT relationships. Exiting intragroup ICT services may interrupt other tech-supported services by the parent organization and remove the ability of the parent to provide sophisticated cybersecurity services which enhance the cyber preparedness of the covered entity
- *Supervision/Oversight*
  Given the breadth of services offered by the parent to the affiliate for daily operations, the parent organization may be considered a concentration risk by the Joint Committee. In the Proposed Text this may further allow oversight of the parent organization by the ESAs. This may create supervisory issues between the national authorities who oversee the parent organization and the ESAs who are expected to oversee the ICT third-party relationships that sit outside of the institutional protection scheme.

While DORA is the first step in a multiphased effort, a solid foundation will serve to support resilience and provide the flexibility needed for Europe's digital finance goals.

Public/Private Partnerships

I believe that sound rulemaking requires feedback from the industry. This allows subject matter experts from both sectors and their unique points of view to be reflected in rulemaking. This creates rulemaking that is fit for purpose and enhances the implementation of measures that promote resilience. EU lawmakers should envisage consultations with the industry to develop technical standards.

It is my hope that clarifying these matters takes a front seat in these discussions. While DORA is the first step in a multiphased effort, a solid foundation will serve to support resilience and provide the flexibility needed for Europe's digital finance goals.

SCOTT MULLINS

Global Head, Financial Services -
AWS Worldwide Financial Services (AWS)

DORA must support digital innovation across the EU financial services industry

The European financial services industry is rapidly digitalising with financial institutions and their customers reaping the benefits of cloud technology, including increased resilience, improved security, and innovation at scale. The EU proposal for a Digital Operational Resilience Act (DORA) aims to introduce a new regulatory framework that will impact how EU financial services institutions work with cloud providers and other critical third parties.

The pace of change in the financial services sector is unprecedented. Financial consumers' expectations are changing at the same pace and new technologies are enabling firms to adapt quickly to address these new needs. As a result, the financial ecosystem is constantly evolving, with new players entering the market and established ones re-thinking their business models. Institutions of all sizes are redefining their approach to business to provide customer focus, agility, and services they need to be competitive and grow.

The cloud has become a critical component of this approach. It allows financial institutions to experiment with new ideas and launch new products and services without the need to invest in expensive and outdates infrastructure, which in most cases cannot deal with the challenges of an increasingly digitalized financial services sector.

Best-in-class technology

In its Digital Finance Strategy, the European Commission is encouraging digital innovation across the sector and many organizations are responding by using cloud technology to transform their businesses. DORA will play a significant part in the Commission's drive for digital innovation, while raising the bar for security, resilience, performance and reliability. Ensuring EU financial services firms are able to access best-in-class technology is absolutely key to delivering this.

It is crucial that the final DORA framework is fit-for-purpose. It must reduce the fragmentation within the EU and across jurisdictions, while supporting innovation and encouraging the adoption of innovative ideas. It must also be robust in managing technology risks. Achieving this will support EU competitiveness in financial services in the long term. A globally interconnected financial system requires coordination and harmonization across jurisdictions. And a similar principle applies to technology. Fragmented requirements will create friction and delay the adoption of the best technology by the financial services sector.

At the same time as DORA is being implemented, the whole sector faces an increasingly complex cyber-threat landscape for which technology is crucial. DORA must harmonise and raise the bar regarding security requirements within the EU. In turn, further efforts are needed at the international level to ensure financial firms don't face duplicative and/or conflicting regulatory regimes.

Vital role for the cloud

The cloud is a crucial enabler for EU firms to develop capabilities in AI, machine learning and other technologies. The cloud model is based upon the highest security standards, meaning all customers benefit from a secure core infrastructure that no single firm would be able to achieve on its own.

AWS is committed to working with the financial community on the implementation of DORA while enabling institutions to deliver agility, seamless interactions and above all innovation.

EU financial firms must have access to the same cloud technology as global competitors in order to maintain a level global playing field and benefit from the highest levels of security available. Cloud technology enables EU financial companies to be resilient and efficient, and supports the digital transformation of the sector.

The work of European policy makers to introduce DORA is a positive and welcome step. AWS is committed to working with the financial community on the implementation of DORA while enabling institutions to deliver agility, seamless interactions and above all innovation. We will continue to support our customers in the EU and globally as they innovate and develop new products and transform their businesses while adhering to the highest security and resiliency standards.

LAURENCE MOLINIER
Director, Risk Advisory - Deloitte

Looking towards the implementation of the EU's Digital Operational Resilience Act

The finalisation of the EU's Digital Operational Resilience Act (DORA) will be an important regulatory development for the financial services (FS) sector this year. Given its breadth and ambition, firms cannot afford to wait for the political process to conclude but should already be considering what successful implementation requires.

The DORA will introduce a new approach to the operational resilience of the sector that streamlines a framework that had previously only existed as a patchwork of EU Regulations and guidelines[1]. This development is in line with a worldwide trend of FS regulators creating dedicated rules for strengthening operational resilience of firms in the sector[2]. The DORA will also introduce the world's first comprehensive oversight framework for Critical ICT Third Party Providers (CTTPs) serving FS clients.

With the EU co-legislator negotiations ongoing, we see several important considerations with regards to compliance challenges and building resilience.

Thinking through implementation in practice

Although the DORA will provide a unified set of requirements for ICT risk management, reporting, testing and third-party risk management, the precise scale of the compliance challenge for firms cannot be fully understood until there is more clarity as to how authorities will implement the new rules.

While many larger firms will have already put in place similar practices for operational resilience or cyber risk management based on existing guidance (e.g., from the European Supervisory Authorities), the DORA goes further. Supervisors may also expect the quality of the work from these firms (for instance, on mapping and identifying vulnerabilities in systems that support critical functions) to be higher due to the systemic role they play in the financial sector. This indicates that the expected two-year implementation period will still be a tight deadline, even for firms with more mature cyber and operational resilience capabilities.

Firms and their supervisors must engage early to discuss not only how they should comply with the DORA's explicit requirements, but to reach a mutual understanding on the desired level of resilience that could be sought for critical functions and business services by the end of the implementation period and after. In our experience, this understanding will be crucial for firms to plan the level of resources and investment needed to meet the expectations of supervisors.

These discussions will also help firms pinpoint areas where building their resilience to the desired level will be more difficult. In a recent executive survey, identifying and managing third party vulnerabilities was highlighted as the most important challenge faced by FS firms in implementing operational resilience requirements.[3] In addition, firms will have to think carefully about medium -term investment decisions, especially in relation to legacy systems, to support their expected level of resilience.

Ensuring international coordination

The operational vulnerabilities and cyber threats that FS firms face do not stop at national boundaries, so regulatory frameworks and operating models should ideally work together. Much has already been done to facilitate this by the Financial Stability Board and the Basel Committee on Banking Supervision (BCBS), and the DORA contributes to this effort.

While this is an important point for the rulemaking process, much will again depend on how supervisors implement the framework and whether work undertaken in one jurisdiction can contribute to meeting requirements in another.

As the DORA moves towards finalisation, FS firms and regulators need to be mindful of the scale of the challenge.

An important case of this will be the approach taken in the ECB's supervision of banks. While the ECB will supervise banks' compliance with the DORA, it is also expected to implement the BCBS's March 2021 Principles on Operational Resilience, an outcomes-based framework more similar in approach to the UK's supervisory-led regime. The 2020 ECB, US and UK authorities' statements, committing to deliver a globally joined-up approach to the supervision of operational resilience[4], demonstrates encouraging cooperation.

While it is natural that regulators with different priorities will put more relative emphasis on the resilience of different operations, there is still significant opportunity for alignment across borders. For instance, it will be important to see to what extent the "important business services" identified by a cross-border firm for its compliance with the UK rules will be allowed to match with the "critical operations" it must identify under the DORA.

Regulators should also work together to ensure that they take compatible approaches to the oversight of Cloud

Service Providers and other CTTPs providing services in the FS sector. While the EU moved first (as the DORA will be the first design and introduction of such a comprehensive oversight framework), the UK and US approaches are due, and may differ in the detail.

Our view is that cross-border FS firms will gain efficiencies when they adopt a consistent approach to operational resilience group-wide and modify it in each jurisdiction as far as necessary to meet specific requirements. Differences between jurisdictional frameworks should not be an insurmountable problem if regulators remain committed to facilitating such an approach and strengthen their coordination of supervisory activity.

The importance of acting... now

As the DORA moves towards finalisation, FS firms and regulators need to be mindful of the scale of the challenge. While a two-year implementation period may feel tight, with a proactive, practical, and collaborative approach there is a real opportunity to implement the DORA in a way that contributes to a more operationally resilient sector overall.

I. Most prominent among these include ICT Risk Management Guidelines from the European Banking Authority and the European Insurance and Occupational Pensions Authority as well as the Cyber Resilience Oversight Expectations from the European Central Bank.
2. Deloitte, EMEA Centre for Regulatory Strategy, International regulatory alignment on operational resilience.
3. Deloitte, EMEA Centre for Regulatory Strategy, 2022 Financial Markets Regulatory Outlook.
4. European Central Bank, Banking Supervision, Statement regarding supervisory cooperation on operational resilience, 2020.

This article has been written by Suchitra Nair and Scott Martin, Deloitte Emea Centre for Regulatory Strategy

EUROFI PRESIDENT // David Wright
SECRETARY GENERAL & PUBLISHER // Didier Cahen
ASSOCIATE PUBLISHERS // Jean-Marie Andrès and Marc Truchet
EDITORIAL COORDINATORS // Virginie Denis and Daniela Craciun
GRAPHIC STUDIO // Initial Production - www.initialproduction.be