CYBER AND DIGITAL OPERATIONAL RESILIENCE

GERRY CROSS

Director Financial Regulation, Policy and Risk - Central Bank of Ireland

DORA – Building on existing principles

The European Supervisory Authorities ("the ESAs") are tasked with jointly delivering the regulatory standards implementing the DORA ICT risk management framework. The Joint Committee of the three ESAs has established a Sub-Committee to deliver these standards and the first batch of Level 2 policy products was launched for public consultation mid-July. Included in the public consultation are four draft regulatory technical standards (RTS) and one set of draft implementing technical standards (ITS).

These technical standards aim to ensure a consistent and harmonised legal framework in the areas of ICT risk management, major ICT-related incident reporting and ICT third-party risk management. The consultation for the first batch runs until 11 September 2023.

The second batch of policy products is expected be launched for public consultation towards the end of this year. Stakeholders in the DORA Regulation are invited to take this opportunity to provide important and valued feedback on the draft technical standards to ensure a solid policy product that is addressing key ICT risks while also being implementable.

The reliance on ICT across all industries is reflected in the development of specific ICT best practice frameworks since 1990. These frameworks have also been used, to various degree, by the financial sector and specific guidance on ICT risk management were issued by the EBA (Guidelines on ICT and security risk management, 2019) and by EIOPA (Guidelines on information and communication technology security and governance, 2020).

The core principles expressed in these guidelines and best practice frameworks focus on the identification of ICT risk, the protection against identified risks, the detection of abnormalities in providing ICT services to the business, the timely response to detected abnormalities and the recovery to normal ICT operation. DORA builds on these existing ICT risk management principles taking proportionality into account.

DORA builds on these existing ICT risk management principles taking proportionality into account.

Implementing DORA and the requirement to identify ICT risk will challenge some firms, especially those with complex ICT systems, as it requires a detailed understanding of the ICT assets and systems supporting business functions. However, in order to adequately protect and ensure the resilience of business services provided to customers, financial entities must first understand what ICT assets support these business functions before they can adequately protect these ICT assets against identified risks.

DORA is also concerned with risks that originates from the provision of third-party ICT services and addresses these risks through detailed ICT outsourcing requirements and by introducing an oversight framework for critical third-party providers (CTTP) of ICT services to financial entities. A public consultation on a Call for Advice (CfA) on the criticality criteria for CTTPs ended in June. Finalising the CfA will take into account the feedback received from more than 40 interested parties before its submission to the EU Commission later this year.

The CTTP oversight framework is currently been developed and the ESAs in collaboration with competent authorities are focusing on the development of organisational structures to deliver the oversight alongside the drafting of the RTS on oversight conduct.

FRANÇOIS-LOUIS MICHAUD

Executive Director - European Banking Authority (EBA)

Addressing dependencies on critical providers through EU oversight

The Digital Operational Resilience Act (DORA) establishes a comprehensive framework on digital operational resilience for EU financial entities. The first pillar of DORA aims at consolidating and upgrading ICT risk requirements that have so far been spread over in different texts of the financial services legislation, to increase operational resilience and foster convergence and efficiency in supervisory approaches when addressing ICT third-party risk in the financial sector.

The second pillar of DORA introduces an EU-wide oversight framework for those providers of ICT services to financial entities that will be designated as critical (CTPPs – Critical Third-Party Providers). This is to ensure that EU financial entities relying on such providers are not exposed to critical risks that may compromise financial stability and the funding the EU economy.

In practice, one of the three European Supervisory Authorities (ESAs – EBA, ESMA and EIOPA) will be designated as Lead Overseer for each CTPP. Oversight activities will assess whether each CTPP has in place adequate mechanisms to manage the ICT risks which they may expose EU financial entities to.

Proper collaboration between the ESAs and EU financial supervisors will be essential. To that end, the ESAs will be setting out a comprehensive cooperation and coordination framework building on the existing institutional architecture enhanced by new structures.

First, the existing Joint Committee of the ESAs that already facilitates cross-sectoral coordination in relation to all matters, including on ICT risk, will be supported by a new Oversight Forum. The latter will bring together representatives of all relevant competent authorities, with steering and consultative powers, to promote a consistent approach in monitoring ICT third party risk and designating CTTPs at the Union level.

Second, the coordination of oversight activities among the ESAs will be performed through a Joint Oversight Network.

Third, at operational level, Joint Examination Teams established for each CTTP will bring together ESA and competent authorities staff to support the Lead Overseers carrying out their oversight activities.

EBA is looking forward to increasing the stability of the EU financial system through DORA.

All in all, the ESAs, competent authorities, resolution authorities, the ECB, SRB, ESRB and ENISA will closely cooperate to enhance situational awareness and identify commons cyber vulnerabilities and risks across sectors. This is in particular reflected in the 'dual mechanism' at the core of the oversight framework: the Lead Overseer will assess whether CTPPs have in place adequate processes to manage the risks posed to financial entities through their oversight activities (e.g. by requesting information from the CTPPs, conducting on-site inspections and off-site investigations and issuing recommendations to CTPPs on its findings) and competent authorities, as part of their prudential supervision of financial entities, may require financial entities relying on the CTPPs to take additional measures to address the risks identified in the Lead Overseer's recommendations.

Due to the inherent cross-border nature of the provision of certain ICT services, the Lead Overseer may also exercise its powers on premises in a country outside of the EU which is used by the CTPP to provide services in the EU. For this purpose, DORA envisages the possibility for the ESAs to conclude cooperation arrangements with third-country authorities.

The DORA oversight framework will require some adjustments from all involved parties: third-party providers servicing EU financial entities, financial entities when managing their ICT risks, competent authorities when rolling out their supervisory toolkit and the ESAs regarding their new oversight functions. Preparations from both private and public sector players are starting now so that the oversight framework be effective when DORA becomes applicable in 2025.

The ESAs are preparing in a joint manner for the implementation of DORA. They are preparing a set of 'level 2' regulatory products (technical standards and guidelines), in accordance with the DORA mandates, of which some have already been published for consultation. They are also launching work on the set of processes and procedures that will be required to operationalise the oversight framework through adequate methodologies and resources.

Increasing the stability and the integrity of the EU financial system through the introduction of the oversight framework is a welcome development, to which the EBA, together with the other ESAs, is looking forward.

DENIS BEAU
First Deputy Governor -
Banque de France

DORA: key conditions for a successful regulatory transformation

The Digital Operational Resilience Act (DORA) is a welcomed development in the EU regulatory framework. It is set to harmonise and increase Information and Communication Technology (ICT) resilience standards and requirements for the whole European financial sector. But it will live up to our expectations only if implemented effectively.

This requires producing high quality texts for the technical standards to be elaborated by ESAs and NCAs, in line with the Level-1 text but also with the state-of-the-art for supervisors and professionals in matters of ICT operation management and cybersecurity. They need to be clear and pragmatic for financial entities and practicable for supervisory authorities (with a high stake in coordination with the various authorities and EU institutions). To this end, feedback from the industry through the public consultations will be carefully considered to have a properly calibrated and usable framework.

Smooth articulation among financial supervisory authorities is also needed to ensure the overall coherence, effectiveness and efficiency of the framework. To that end, the roles of different designated and competent authorities will need to be clarified for determining the scope of entities subject to threat led penetration tests (TLPT) and leading such exercises.

The efficient functioning of the pan-European coordination framework for cyber-crisis within the financial sector (named EU-SCICF), to be set up by the ESRB, will also need to be ensured. Going further, a full cooperation between authorities in charge of the DORA and the Network and Information Security (NIS2) frameworks is also needed at Member State level. For instance, the NIS authorities still need visibility on major ICT incidents affecting the financial sector, and should assist NCAs in handling incidents or crisis, providing their technical expertise.

A good illustration of these implementation challenges is the new oversight model for critical third-party providers (CTPP). The assessment of the risks arising from critical providers (in particular the ones established outside EU) is a new mandate for public authorities.

This is the most observed piece of the DORA regulation from outside Europe. The new framework has to deliver significant results, and supervisors need to be empowered with all the necessary tools to make it so. The upcoming operational framework should reach the ambitious level of oversight set by DORA.

As DORA marks a breakthrough, its implementation requires clear and effective secondary legislation.

On-site inspections are a key tool for guaranteeing that critical service providers meet DORA's requirements and comply with the requests of the Joint Examination Teams. In that sense, they should not be reduced to mere 'courtesy visits' and should rather align with the intrusive model followed by the SSM for bank inspections.

Another key question relates to the providers that will be designated as critical. It is important to identify the critical providers supplying the ICT services that pose the most important risks. The criticality is not merely size-based and the sensitive nature of the ICT services should be considered.

Finally, the supervisors will also have to assess whether the clients of the CTPPs duly strengthen the management of their third-party risks and resort to all their contractual powers provided by DORA.

National supervisors will have to upscale their internal resources for this new role. Scarcity of talents in IT and cyber risk management will pose a challenge for all authorities.

A condition for success will be to embrace a cooperative approach. As far as possible, ICT tools, human resources and information channels should be pooled among domestic and EU supervisors to avoid unnecessary duplications. Domestic supervisors have experience in terms of ICT-risks monitoring and this experience needs to be fully leveraged for establishing an efficient oversight framework.

GIUSEPPE SIANI

Director General, DG for Financial Supervision and Regulation - Banca d'Italia

The long path for digital resilience

Technology and ICT risks have overtime assumed an increasing importance for regulators and supervisors as well as for financial entities, due to endogenous and exogenous drivers.

As to the former, technological innovation influences significantly business models and the strategical decisions of financial entities: digitalisation and cloud computing are modifying the way they operate, thus providing new opportunities to satisfy clients' needs, reducing internal costs and improving internal processes. In several cases the operational model is entirely based on technology: this is the case for example of the so called *challenger banks*. Hand in hand with digitalisation, also the dependence on ICT providers and the interconnection among financial entities increase. Technology provides opportunities but also operational, legal and reputational risks. In addition, ICT providers can represent a single point of failure given that one incident can spread over the system.

As to the latter, irrespective from the financial entities decisions, the eco-system they operate has changed materially too, due to the technological innovation itself, given for example the increasing number of cyber-attacks and the rising of frauds to customers mostly based on social engineering. These exogenous elements should therefore be factored into business decisions too in order to properly manage IT/cyber risk and, eventually, preserve data integrity.

The NIS2 Directive, the general ICT risk regulation, and DORA, the financial sector Regulation, address endogenous and exogenous ICT risk factors; they also introduce a cross-sector and cross-country harmonised framework aimed at enhancing ICT security. Both regulations take into account principles and technical standards that have long been used in the financial sector – thus incorporating lessons learnt from the past - and integrate them with safeguards for new risk factors; for example, DORA is not limited to ICT risk but also addresses those new risks that arise from third parties thus introducing an oversight regime for the critical ICT providers.

An interconnected world requires global rules for cyber and operational resilience.

Despite the comprehensive package, DORA is a principle based regulation that can be implemented by the financial entities according to their size and risk profile; DORA also provides for a simplified regime for the smallest and less interconnected entities and some limited discretions at national level to address proportionality. It will be then the (not new) challenge of supervision to understand if the concrete implementation of DORA from the entities in scope is consistent with the financial entity risk profile, actually applying the proportionality principle. Some significant challenges still need to be addressed:

1. **Legislative process:** DORA requires the completion of the regulatory process in 18 months, which must absolutely be complied with;

2. **Cross sector harmonisation:** DORA provides uniform rules for any financial entities regulated by the European legislation, from the traditional banks to new crypto asset providers. To guarantee the overall system resilience, as national authorities, we should apply the same ICT security principles as provided by DORA even to those financial entities, regulated according to the national legislations, not in the scope of DORA[1];

3. **Oversight regime of critical TPP:** the oversight regime will imply a complex interaction among authorities: we must design an effective cooperation framework, as it is key for successful implementation;

4. **Harmonisation of supervisory methodologies:** having a common regulatory framework among countries and sectors is not enough: it is necessary to develop common methodologies, under the ESAs coordination, to ensure consistent implementation.

What further issues remain? In an interconnected world, we need global rules and common principles for cyber and operational resilience. It is therefore important to leverage on the ongoing work of the international standard setters to assess whether common requirements are properly implemented and the risks consistently supervised; a lot has already been done, but we should never lower our coordination efforts

This looks particularly key in the case of cyber-attacks: should unfortunately a cross jurisdictional event occurs, all the community (financial entities, authorities) should be prepared: we have made a lot of progress at the international level (e.g. within the G7 countries and the EU) developing systemic cyber incident coordination frameworks. But we still need to work on this topic defining common incident reporting frameworks, secure communication channels among authorities, conducting more case simulations on different adverse scenarios and developing cyber incident response plans.

1. *As an example, among the others, I refer to financial companies specialised in consumer credit, leasing and factoring.*

MATTHEW MARTINDALE
Partner, Cyber Security - KPMG LLP

Targeting strategic resilience

For several years now, operational resilience has been at the top of the regulatory agenda for financial services. Understandably so, with regulators acutely aware of the threat of disruption to financial firms, and by extension to their customers, particularly in times of stress. They also recognise that in the digital age, the interconnectedness of the global financial system means that disruption can spread rapidly.

Underpinning the many regulatory initiatives is the common desire to create a financial services sector that is more resilient to disruption, reducing the risk of wider contagion, financial instability, harm to end-customers and reputational damage.

Firms are operating in an environment that has long been in a state of simultaneous and overlapping crises. All signs indicate that polycrisis is the new normal. The question firms need to now ask themselves is not 'if' but 'when' will the next crisis strike? And when it does, will they be positioned to remain worthy of their stakeholders' trust?

Firms that recognise this opportunity and invest in building a strategic operational resilience capability will gain a significant competitive advantage over those who view it as just another compliance exercise.

Cyber and ICT security risks are greater than ever due to the accelerated adoption of technology and increasing sophistication of external bad actors. The regulatory response has included the Network and Information Security (NIS2) Directive and the Digital Operational Resilience Act (DORA). But developing rules and regulation is one thing – making them work is another.

So, what do we mean when we talk about successful implementation of DORA and NIS2? And where do the challenges lie for firms and regulators?

KPMG member firms are working with clients to prepare for new requirements and to help them create future-aware resilience cultures. Key to this is the conviction that it is possible to develop a single strategic resilience capability that can meet the needs of multiple regulations and jurisdictions.

The starting point is the plethora of regulation that firms must deal with, at a local, regional, and global level and across different disciplines, including many legacy regulations. We know that across this patchwork of regulation not all the requirements will be aligned, therefore it is critical that firms take a wide view and focus on the big picture.

Proliferation of rules-based regulation should be considered an enemy of strategic coherence.

Much is made of the complexities and nuances of different sets of requirements - these are important as they translate to real costs and implementation challenges for firms. Taxonomies vary, for example, between EU and UK definitions of 'important' or 'critical' functions. DORA and NIS2 also have a stronger focus on technology assets, that must be made more resilient to ensure continuity of service, than on other capabilities. In other areas, such as critical third parties, there is less divergence – requirements relating to lifecycle and criticality criteria are broadly similar in DORA and the equivalent UK regulatory proposals. However, there are potential complexities within the EU itself, where DORA's focus on technology vendors may present challenges due to the necessary uplift from the EBA guidelines on outsourcing to DORA's coverage of all third parties.

However, to focus only on where discrepancies lie risks focusing only on compliance and not on improving resilience in the system. Regulators have a role to play here in ensuring interoperability between rules and sufficient convergence so that firms can take a pragmatic approach.

There is also a continuing debate on whether prescriptive or principles-based rules are most appropriate. Again, coming from the perspective that developing enterprise-wide resilience must be the goal, prescriptive requirements run the risk of becoming very compliance driven. The proliferation of rules-based regulation in the resilience space should be considered an enemy of strategic coherence – the real prize is strategic resilience.

Elevation of the resilience agenda to board and ExCo level is a welcome and necessary development. Firms should take an enterprise-wide approach - considering technology, cyber security, data, people, third parties and facilities within their organisation and across the supply chain – to deliver real resilience.

The quest for resilience, whether from technology or business process perspectives, will fail if responses are mobilised in silos. Regulators and firms must increasingly recognise the interlinkages across the industry and into the wider economy. NIS2 brings strategic integration across sectors and industries, picking up non-regulated providers and demonstrating again the broader theme of integration and connectedness. As it becomes increasingly difficult to know what 'financial services' is and where it begins and ends, greater connectivity is required to provide a secure ecosystem.