CYBERSECURITY AND DIGITAL OPERATIONAL RESILIENCE

GERRY CROSS
Director Capital Markets and Funds – Central Bank of Ireland

DORA – a new era in digital operational resilience

Since 17 January, Europe's new Digital Operational Resilience Act has been live. DORA is a new style of "ecosystem" regulation, representing a multifaceted approach to digital operational resilience. DORA is a good example of regulatory simplification with its focus on outcomes rather than rules.

While a small number of policy products are still going through the legislative finalisation process, most of the technical standards that provide DORA's implementation details have come into effect. This significant task, completed by the three European Supervisory Authorities (ESA) together with more than 40 national competent authorities (NCA) and other agencies, has demonstrated that effective outcomes-focused collaboration can deliver harmonised, proportional and high-quality financial regulation for Europe.

Now that DORA is live and being implemented by financial regulated entities, convergence of supervisory approaches to implementation will be important. This should seek to ensure that DORA's harmonised cross-sector approach is appropriately reflected in implementation by the more than 40 national authorities. This will not be an easy task, but good engagement and discussions are underway at ESA and NCA level to ensure just that.

That DORA is indeed live can be seen in ICT-related incident reporting which is now under way. Incidents are now being reported across the Union as required and the ESAs as well as NCAs are monitoring and analysing these closely. This will over time transform knowledge, preparedness and responsiveness.

In April, financial regulated entities subject to DORA will have to submit the Register of Information (RoI) of contractual ICT services provided by third-party providers and this will form the basis on which the ESAs will identify and designate the most critical ICT services provided by third-party providers.

The supervision of financial regulated entities in accordance with DORA will take time and has to fit in the respective supervisory engagement plan of a given financial regulated entity. This of course means that financial entities will be assessed at different times, similar to supervisory engagements for other outcomes.

DORA is a good example of regulatory simplification with its focus on outcomes rather than rules.

An important topic continues to be financial oversight and monitoring of the outsourcing chain. The initially proposed level 2 requirement in this regard was ultimately omitted from the level 2 regulatory technical standard on technical legislative grounds. It will nonetheless remain essential for firms to ensure effective oversight of all their outsourcing arrangements on an ongoing basis.

FRANÇOIS-LOUIS MICHAUD

Executive Director – European Banking Authority (EBA)

DORA: focus on the first months of application

DORA is a breakthrough in financial regulation and supervision. For the first time, the requirements on digital operational resilience, which were spread across different legislations, are now streamlined through a single, harmonised framework for all regulated financial entities.

DORA addresses in a comprehensive and consistent way cyber risks, vulnerabilities, and the dependency of the financial sector on technology companies. As these risks are evolving fast, fastly, good risk-based supervision requires us to be forward-looking and to anticipate future issues coming into our way. In recent months, banks have been suffering from Distributed Denial-of-Service (DDoS) activity linked to geopolitical events, a surge in mobile banking trojans, and an increase in the complexity of the attack vectors. Data breaches through fraud, supply chain attacks, social engineering campaigns and politically motivated hacktivism also remain prominent drivers behind cyber threats.

All this suggests that we cannot be complacent. While it is clearly early days to draw the first lessons from the implementation of DORA, the EU financial sector's investments in ICT security infrastructure may start bearing some fruit. The number of successful attacks resulting in a major ICT-related incident in autumn 2024 has not risen further compared to spring 2024 in spite of increasing sophistication and a continued high number of attacks.

After three months of DORA application, some other considerations can already be drawn.

Firstly, DORA started applying in January 2025 and did not provide for a transitional phase. However, its requirements are not entirely new per se. Indeed, they leverage on existing sectoral legal practices and expectations. In the banking sector, a lot of work had already been done as a response to EBA's guidelines on outsourcing, on ICT and security risk management, on incident reporting. Banks have been accustomed to this for years. For them, the bulk of the adaptation to DORA consists of translating previous requirements and filling some gaps.

Efforts for smaller institutions to comply with DORA may admittedly be higher as they have so far been subject to less demanding sectoral requirements. Still, they have an important role to play to offer to clients and the EU economy as a whole a good level of resilience. With this in mind, supervisory expectations will vary depending on the size and overall risk profile, and the nature, scale and complexity of services, activities and operations of each financial entity, assuming that the risks have to be properly mitigated by all of them in any case.

DORA: a milestone to streamline & strengthen the approach to ICT resilience for EU financial sector.

Secondly, in a statement published at the end of 2024, the three ESAs identified the areas for increased attention from financial entities in the first months of DORA application. The effective management of ICT-related incidents is a cornerstone of DORA, as it can help identify threats and address vulnerabilities. Banks should be equipped to record, classify and report their major ICT-related incidents, and to follow-up properly. Supervisors report these major ICT-incidents to the ESAs, which can thus have a comprehensive overview on the ICT threat landscape. During the first eight weeks of reporting, the EBA received reports on more than 500 incidents, affecting mostly IT systems, payment services and on-line banking.

Moreover, in the context of their third-party risk management, banks will need to have ready their registers of contractual arrangements for competent authorities. The latter will share them to the ESAs by 30 April 2025 to designate critical third-party ICT-providers (CTPPs), which will be placed under the ESAs oversight. ICT resilience being a cross-sector issue by nature, the ESAs created a common oversight function, to maximise efficiency, simplify reporting and coordination issues and ensure consistency.

Financial entities can prepare leveraging on ITS on the Register of Information and on the 2024 ESAs dry-run exercise, which showed that while a very large number of financial entities were already prepared or well advanced in their preparations, others need to intensify their efforts. Data quality should improve across the board, to ensure this register is a relevant third-party risk management tool for the financial entities themselves.

Going forward, the ESAs will also support supervisory convergence across the EU, to ensure a consistent approach in supervising DORA and related policy instruments. This will contribute to a level-playing field, legal certainty and transparency for financial entities, ICT third-party service providers and competent authorities, thus enhancing EU's resilience and competitiveness.

FRANCESCO MAZZAFERRO
Director General of Secretariat – European Systemic Risk Board (ESRB)

Preparedness is key to financial sector resilience

Since 2017, the ESRB has been working on systemic cyber risk in the EEA and identified key features of how a cyber incident of sufficient speed and scale can propagate through the financial system and threaten financial stability. The financial system performs a number of key economic functions which support the real economy and heavily relies on robust ICT infrastructure for the continuous delivery thereof. The increasing digitalisation of financial services in combination with the presence of high value assets and data make the financial system vulnerable to cyber incidents.

Core vulnerabilities are either idiosyncratic – unique to each individual entity – or common – prevalent or similar across the system. Common vulnerabilities are for example insufficient oversight of widely used ICT third party service providers (ICT TPPs) and the supply chain (which is now an excellent cornerstone of DORA), inadequate cyber hygiene or lack of investment in cyber threat intelligence and cyber security. Such vulnerabilities may be exacerbated through high interconnectedness and non-substitutability of actors and services once an incident occurs.

The motive behind malicious cyber activity depends on the threat actor. Cyber criminals' main goal is profit seeking and sometimes political activism while nation state's primary objectives are covert reconnaissance, projection of power and sometimes overt destruction of critical infrastructure or retaliatory action within the geopolitical context; to some extent overt action follows covert espionage. What all actions, however, have in common is that cyber risk does not respect borders and moves in different ways and across layers of the system than traditional financial risk. This makes it inherently difficult to quantify.

The ESRB's primary focus has been on (i) the potential impact of a systemic cyber incident, (ii) all actors' preparedness and (iii) the system's resilience as a whole.

At all times, it is essential that both, authorities and the private sector share information on vulnerabilities and in case the risk materialises, related incidents. DORA provides a structured and cross-sectoral framework for the sharing of incidents. However, to increase the level of preparedness, also information sharing beyond existing incidents should be continuously fostered and seen as an integral part of our collective approach to cyber resilience. To raise the general level of awareness, the ESRB has continuously been advocating for that.

> **No entity in the financial system exists in isolation and thus carries a distinct responsibility.**

To raise the level of preparedness, the ESRB developed a framework for cyber resilience scenario testing (CyRST). This framework guides macroprudential authorities in their pursuit to test the financial sector's resilience and preparedness. In this setting, testing as many dependencies as possible is crucial and financial entities need to be aware of their place in and effect on the financial system. The scenario should focus on the impact of the system-wide cyber incident on firms and how they manage their response and recovery, rather than the detailed technical factors that caused the incident. The scenario would ideally be uniform and apply to all firms involved and thus support a system-wide assessment thereafter. This high-level framework has already been adopted by several authorities in the EEA and the number is continuously growing every year.

In the event of a crisis, cooperation and coordination frameworks are essential to minimise a potential coordination failure. In 2021, the ESRB recommended the European Supervisory Authorities (ESAs) to develop a pan-European systemic cyber incident coordination framework (EU-SCICF) alongside DORA. This framework is now operational and will be key in assessing financial stability implications during a cyber crisis. Cooperation within a country, between countries and in global networks is essential. Therefore, the EU-SCICF gathers all relevant actors in the EEA and acts as bridgehead to other frameworks.

From a macroprudential perspective, the development of cyber maps for the entire system would greatly benefit our understanding of systemic cyber risk. On one layer, the financial system with all its connections such as interbank and payment systems. On a layer below, one must consider all technological dependencies, ICT TPPs' interconnectedness among each other and with the financial sector. This could give us a better understanding of how cyber risk truly moves through the system and enable macroprudential authorities to act accordingly. In the end, no entity in the financial system exists in isolation and thus carries a distinct responsibility in the overall system's resilience. However, a common approach to data sharing among the supervisory community is essential in our collective effort.

ULRIK NØDGAARD
Governor – Danmarks Nationalbank

Cybersecurity and digital operational resilience: pending and emerging issues

The cyber threat is pervasive, exacerbated by the geopolitical situation, and ever-presently manifested via state actors and organized criminal groups with increasingly advanced capabilities. The financial sector plays a critical role in society, and advanced cyberattacks against financial institutions or payments systems have the potential to threaten financial stability on a systemic level.

Strengthening cyber resilience is complex work and requires continuous efforts along many fronts, both within individual entities and collectively. At Danmarks Nationalbank, we have prioritised work on cyber risks in collaboration with the financial sector since 2016. The financial sector's joint work on cyber risks takes place within the framework of the public-private collaboration forum FSOR, Financial Sector Forum for Operational Resilience, initiated by Danmarks Nationalbank nine years ago. FSOR is chaired by Danmarks Nationalbank and participants include systemically important banks, data centers, owners of critical payments infrastructure, representatives from insurance and pension sectors, and key authorities.

FSOR has initiated a series of mitigating measures that can be described as two waves. The first wave concerns preventive measures, while the second wave focuses on contingency measures. Among the preventive measures are threat-based red team testing of entities in the financial sector under the TIBER-DK programme. TIBER tests take place in live production environments, i.e. in the critical systems that are used to support the daily activity in the financial sector. In a TIBER test, the entity is to identify, prevent and respond to advanced cyberattacks from ethical hackers – a so-called red team – to gain learning on protecting societally critical activities against cyberattacks and preventing the cyberattacks from causing damage. Danmarks Nationalbank was among the first central banks to implement TIBER, building on a framework developed by the European Central Bank, ECB. In Denmark, many tests have been conducted since 2018, and this has generated crucial learning serving to strengthen cyber resilience across the Danish financial sector. The Digital Operational Resilience Act, DORA, establishes threat-led testing, TLPT, as mandatory for significant financial entities in the EU. Danmarks Nationalbank is the authority for TLPT in Denmark.

Another preventive measure facilitated by Danmarks Nationalbank is the regular mapping of cyber maturity in the financial sector. The mapping is done via surveys conducted among FSOR members to gain insights into the sector's self-assessment of its cyber resilience, creating important learning and the opportunity to benchmark against peers.

Strengthening cyber resilience is complex work and requires continuous efforts along many fronts.

Although the Danish financial sector has significantly increased its cyber maturity over the past decade, it is not possible to fully protect against and prevent all cyberattacks. Among the initiated contingency measures is the establishment of a joint crisis response among FSOR members, the FSOR Crisis Management. In case of a severe cyberattack, coordination between FSOR members and communication to the public is key to contain the incident and handle reputational risk. FSOR Crisis Management is regularly tested to ensure that it is efficient functioning.

Another initiative to enhance crisis management and business continuity is the collaboration between the Danish Financial Supervisory Authority and Danmarks Nationalbank on a stress test of operational resilience at the sector level. The starting point is that an incident has occurred, and the companies' cyber defenses have been breached. The purpose of such tests is to examine how individual entities handle a large-scale, long-term operational IT incident in collaboration with other companies in the financial sector, FSOR's crisis management, and authorities. The results can shed light on the need for additional mitigating measures to increase operational resilience in the sector.

Furthermore, we are working towards a long-term payment contingency measure in Denmark, increasing the number of payment cards that can be used off-line to ensure basic consumption for at least a week.

Considering the geopolitical situation and the maturity of the Danish financial sector, Danmarks Nationalbank are also working on business continuity and recovery measures in extreme but plausible scenarios. The work should result in recommendations on how the financial sector can prepare for such scenarios and continue to carry out the most societally critical activities if damage has occurred.

The cyber threat landscape is constantly changing, and both entities and authorities must continuously evolve with the threat to stay ahead of developments. It is therefore crucial to continue work on strengthening cyber resilience through both preventive and contingency measures.

VINCENT MAAGDENBERG
Chief Risk Officer – Rabobank

Strengthening resilience: Lessons from DORA implementation

The Digital Operational Resilience Act (DORA) aims at a situation where EU financial entities can withstand and handle significant ICT disruptions. Its implementation this year has doubtlessly raised the resilience level and aligned them with customer expectations, as most customers have become fully dependent on digital banking systems. The interconnectedness with the economy of bank apps and related financial systems means disruptions can have cascading effects, highlighting the need for comprehensive resilience strategies. DORA is a good start, but more is needed.

The requirements in DORA are not entirely new, as they build on the 2019 EBA Guidelines on ICT and Security Risk Management. In the Netherlands, Dutch law also has required banks for years to perform systematic ICT risk analyses and to have clearly formulated policy principles for managing outsourcing risks. Therefore, banks did not have to start from scratch, though DORA made explicit what banks were already required to do. Furthermore, DORA expanded the scope by including more critical service providers, which is a positive and necessary development given the increasing interconnectedness.

One item that DORA now makes explicit is the importance of collaboration with all critical ICT providers. Although for some of those providers a robust partnership approach was already in place, DORA ensured that the framework is also implemented with those critical ICT service providers where this was not yet existent. This certainly strengthens digital resilience and fosters continuous improvement and proactive risk management. Also the shift to thinking in end-to-end (product) processes and not solely at individual applications contributed to resilience. Here we have also leveraged existing regulations namely the Bank Recovery & Resolution Directive to determine which processes are critical and important. In this way we have made maximum use of what existed already with the new Act coming into play.

This process also highlighted the necessity for comprehensive training and awareness programs fostering a resilience-focused mindset throughout the organization.

Given our critical role in the economy, banks also have a responsibility to assist their clients. We noted that clients appreciate banks that proactively inform them on how to achieve and maintain digital resilient. For instance, SMEs are particularly vulnerable given their relatively small size, lack of ICT knowledge and outdated infrastructures with weak security protocols. Without taking over responsibility, we are now actively informing our SME clients to mitigate these risks.

> **In becoming digital resilient DORA is a good start, but more is needed.**

Besides working on their digital resilience as envisioned by DORA, the banking sector is also witnessing new trends such data centralisation, cloud computing, outsourcing, (Gen) AI and quantum computing. In addition to what DORA is requesting it's therefore important that banks, critical ICT financial service providers and their supervisors leverage technology and AI to combat cyber-risk. More enhanced cooperation and openness about the exchange of cyber threats, lessons learned, and best practices is needed as it can play a crucial role to remain top in class. Regulatory bodies can support these efforts by providing clear guidelines. However, the challenge is that we must warrant that this information does not fall into the hands of cybercriminals. This would be significantly counterproductive to the efforts made.

On top of what DORA requires, recent geopolitical trends also makes it essential to prepare for scenarios, playbooks and the frequent testing of them where hybrid threats make that banking apps do not function. This underscores the need for not only financial institutions but also energy suppliers, telecom operators, and other vital processes in our economy to become more resilient against military and hybrid threats while maintaining a robust democratic framework. This requires a shift in thinking and behaviour across all sectors of our society.

Given these threats and high dependency on digital infrastructures, it would be beneficial for the European Commission, Member States, EU supervisors, banks, payment service providers and other relevant critical ICT service providers to explore ways to enhance resilience together. To mitigate the risk of a total fall-out, one could think about the setting up of a crisis runbook at national level for the most critical banking services to mitigate the risk of not having access to current accounts and payment processing, which are essential to our customers and the (regional) economy. First at national level and thereafter expanding to European level.

In an unstable world banks play a crucial role in protecting the financial infrastructure, supporting society and facilitating employees to be prepared to enable them to play an important role in crisis situations. This is what our clients expect from us.

FENITRA RAVELOMANANTSOA
Head of Cloud Regulatory Affairs, EMEA – Google

DORA oversight: fostering a collaboration is a key

The Digital Operational Resilience Act (DORA) is now in effect, setting a new course for the EU financial sector. Google Cloud, alongside our financial services customers and regulators, has been actively engaged in DORA readiness preparations since the requirements were finalized in 2022, and early experiences offer valuable insights.

A primary lesson is the huge importance of proactive and open communication and transparency during both the draft regulation and the implementation phase. As the CTPP oversight framework is novel, we believe that a dialogue between regulators, financial entities, and ICT providers is key. We believe we are on the right track to continue this transparent exchange.

To directly support customers and ensure transparency, Google Cloud has taken concrete steps: updating our contractual terms in February 2024 , providing clear mappings for both Google Cloud and Google Workspace to help customers understand how our contracts, controls, and processes support their compliance efforts. We've also published essential resources, including the DORA FAQs, an ICT Risk Management Customer Guide, the Register of Information Customer Guide and the Third-Party Risk Management Resource Center. These resources provide critical information on our risk management practices, subcontractor management, and the necessary data for customers to complete the relevant Register of Information templates for Google Cloud services.

DORA marks a pivotal moment for the tech and financial ecosystem. This represents a fundamental shift in financial regulation, with the European Supervisory Authorities now positioned to shape the oversight rules directly governing ICT providers.

As the first challenge, it's crucial to acknowledge that ICT providers operate differently to financial entities. These differences, including organizational structures, development cycles, and service delivery models like the shared responsibility model in cloud computing, may be significant. The regulators have an unique opportunity to establish an oversight framework focused on achieving the desired resilience outcomes, while allowing flexibility in how tech companies achieve them. For example, requirements related to internal controls or audit processes may need to be tailored to the cloud environment, recognizing the shared responsibility model and the continuous delivery of services. Regulators should also be mindful of the rapid pace of technological change and design frameworks adaptable to future innovations. Recognising the dynamic nature of cloud technology, Google Cloud is committed to collaborating with regulators more broadly by sharing our technical expertise and insights.

> **DORA' marks a pivotal moment for the tech and financial ecosystem.**

Another major consideration is the consistent interplay between European and national supervisors, when CTPPs are being directly overseen and indirectly as an ICT provider to supervised financial entities, to avoid potentially conflicting views. For example, differing views on specific provisions can lead to confusion and delays. To mitigate this, continuous cooperation between European and national authorities is crucial, alongside a focus on desired outcomes rather than overly prescriptive methodologies.

To effectively combat cyber-risks, market participants and supervisors can further leverage technology and AI through enhanced cooperation and the exchange of best practices. Promoting industry-wide information sharing is crucial, with DORA outlining considerations for voluntary sharing of cyber threat intelligence. Establishing common standards for data sharing would also enable a more effective response to cyber threats and operational disruptions.

AI offers significant potential for the industry, and Google Cloud integrates AI into its cybersecurity strategy, using machine learning to automate security tasks and enhance response capabilities. Mandiant, now part of Google Cloud, provides expertise in threat intelligence and incident response, complementing AI capabilities. As a leader in cybersecurity, Google Cloud is committed to continuing to share our knowledge and expertise with both financial institutions and regulators to enhance cybersecurity across the industry. Google Cloud has used its experience as a leader in the security field to provide thought leadership to support the development of pooled Threat-Led Penetration Testing (TLPT). These efforts are all aimed at fostering a greater understanding of the technological landscape and addressing evolving cyber threats.

Lessons learned from DORA implementation by Google Cloud and its financial sector customers highlight the importance of open and early dialogue between the stakeholders. In terms of achieving DORA's objectives, it is still early days, but we are confident that with support and collaboration between stakeholders, the digital operational resilience across the European financial sector will be significantly enhanced.