Cybersecurity and digital operational resilience

1. Progress of DORA implementation

1.1 Implementation of DORA in the EU

The Chair noted that the Digital Operational Resilience Act (DORA) framework became applicable in January 2025. The approach for developing the DORA Regulatory Technical Standards (RTS) has been pragmatic and rapid, taking around two years to deliver. Implementation is proceeding on schedule. Incident reporting is in place and convergence in supervisory practices across member states has been observed, facilitated by the joint efforts of the European Supervisory Authorities (ESAs).

A regulator confirmed that the early implementation stages of DORA are progressing well. Industry and supervisory authorities are both making significant advances. A dry-run exercise conducted in summer 2024 helped financial entities to prepare for the production of their registers of information. The ESAs will receive this data for the first time by the end of April 2025. While variations in quality are expected, this will be a key input to enable the identification of critical ICT third party providers (CTPPs).

Contractual adjustments are also needed. Although institutions have had to comply with these requirements from January 2025, supervisors are currently taking a proportionate and balanced approach to oversight. The new harmonised incident reporting framework is already operational and is enabling more efficient dissemination and coordination of information. Supervisory authorities, including ESAs and the National Competent Authorities (NCAs), are increasing their internal oversight capacity and hiring new staff. Methodologies have been developed and recruitment is ongoing, with proportionality factored into approaches.

The implementation of the new oversight regime for CTPPs is proceeding as planned, the regulator added. This model, similar to that used for payments, relies on close cooperation between authorities and stakeholders to ensure consistent expectations and effective risk management across the entire financial ecosystem. Formation of the Joint Examination Teams (JETs), which will lead on the oversight of CTPPs, is underway, with operations expected to begin by the end of 2025. The designation of CTPPs is due to begin after summer 2025, once relevant data is collected. Engagement with potential CTPPs has already begun informally and will intensify ahead of formal designations in November.

An industry representative shared the perspective of a cloud service provider (CSP) on the implementation of DORA. Collaboration between regulators, financial firms, and ICT providers is key to enhancing operational resilience in the European financial market. The speaker's firm has been preparing for DORA since 2022. The main focus so far has been on equipping clients with the tools and information needed for their own compliance. Contracts have been updated to align with DORA's Article 30 requirements, and customer guides on ICT risk management and information registers have been published. Additional support includes a third-party risk management portal and a DORA FAQ page addressing the main questions around compliance with DORA.

Another industry representative agreed that good progress has been made in the monitoring ICT outsourcing. The delay in publishing the RTSs initially caused ICT service providers to pause moving forward with the implementation, but momentum is building, and implementation is now well advanced.

1.2 International cooperation

The Chair emphasised that international cooperation remains essential in the evolving global threat landscape and should be reinforced through deeper cross-border dialogue. The work of international bodies such as the Financial Stability Institute (FSI), Financial Stability Board (FSB) and Basel Committee to ensure consistency also supports effective cross-border dialogue, particularly through a focus on practical operational risks in today's challenging environment.

A regulator reported that, from the outset, the ESAs engaged with non-EU jurisdictions, such as the US and the UK, to share experience on risk mitigation practices and how qualitative and quantitative approaches can be appropriately balanced. These exchanges helped refine DORA and ensure coherence with global practices. As geopolitical risks are increasing, strong cross border cooperation remains a cornerstone of effective cyber resilience. The visibility of critical ICT vulnerabilities and dependencies enabled by DORA creates a solid foundation for building better informed responses and increasing cooperation both within the EU and internationally.

2. Main benefits of DORA

The Chair summarised that DORA is an innovative, outcome-focused piece of legislation designed to enhance digital resilience across the entire financial ecosystem, not just for a specific category of players. Instead of imposing detailed rules, DORA provides a flexible framework aimed at delivering tangible results in areas such as risk management, outsourcing, threat-led penetration testing, incident reporting, and oversight of cloud and third-party providers.

A regulator emphasised that DORA is a breakthrough in terms of content and approach. DORA is a cross-cutting framework that applies to all financial entities in the European financial ecosystem and addresses all the

dimensions of ICT resilience. Its implementation is harmonised across all 27 member states, streamlining previously fragmented practices and creating a systematic approach to digital resilience. The collaborative nature of the implementation of DORA, with all three ESAs working jointly is also a novelty. This coordination reflects the cross-cutting nature of digital operational resilience, which affects not just banks but all types of financial institutions. However, for many firms, while aspects such as incident reporting and contractual clauses may evolve, the underlying risk management principles will remain unchanged.

A central bank official remarked that DORA is a timely initiative that will contribute to strengthening awareness of cyber risks and the need for cyber resilience across the whole financial sector. While large systemic banks are already well-equipped to address cyber risks, this is generally not the case for smaller banks and pension institutions. DORA will have a particularly significant impact on these smaller institutions. In Denmark, smaller banks often depend on shared IT service providers. DORA clarifies governance structures and responsibilities within these shared arrangements, contributing to a reduction in associated risks. DORA has also prompted discussions around the applicability of threat-led penetration testing for pension institutions, which are a major component of the Danish financial system. Following detailed deliberations, regulators concluded that pension funds should be subject to such testing, which is expected to become mandatory once the relevant RTSs are finalised.

3. Improvements needed in the implementation of DORA

3.1 Aligning DORA and financial regulatory frameworks

An industry representative noted that DORA does not introduce radical changes but requires institutions to reassess their digital operational resilience across entire value chains. One challenge is the lack of harmonisation between regulatory regimes, such as between DORA and the Bank Recovery and Resolution Directive (BRRD), particularly in the definition of critical processes. To ensure continuous operation of essential services, alignment of these definitions is vital. Using the BRRD for scenario analysis in operational resilience remains difficult, as the directive is primarily focused on capital and liquidity and, unlike European Banking Authority (EBA) stress tests, it does not provide a clear pathway to concrete action.

3.2 Streamlining supervisory activities for CTPPs

An industry representative emphasised that the impact of the CTPP oversight regime must be carefully assessed. Implementation of this regime will require close coordination between supervisors, ICT providers and financial institutions. As a new and untested framework, it may introduce additional layers of complexity. One key challenge is the dual oversight structure of direct oversight of CTPPs by the ESAs combined with indirect supervision by NCAs via the financial institutions that use CTPP services. Clear expectations and consistent approaches between these supervisory levels will be essential. It is also crucial to differentiate between traditional financial institutions and technology providers in the operational application of oversight. Supervisors need to develop a strong understanding of technology-specific concepts, such as the shared responsibility model in cloud computing. An outcome-based approach that enhances resilience without hindering innovation through overly prescriptive measures should be prioritised

The Chair agreed that, as the implementation proceeds, CTPP oversight and traditional financial supervision must be effectively coordinated to avoid both duplication and regulatory gaps.

In response to the comments regarding the complexity of the dual oversight regime, a regulator acknowledged the potential concerns raised by the interplay between traditional supervision and the new DORA oversight regime. Efforts are being made to align supervisory activities and share information to minimise duplications and burdens, especially on third-party providers.

3.3 Improving the proportionality of DORA

An industry representative observed that the implementation of DORA within banking groups poses potential proportionality issues. All legal entities within a banking group must comply with DORA equally, even very small subsidiaries, which increases the complexity of implementing the framework. There should be greater sensitivity to the size of different entities within a financial group.

A regulator acknowledged that, although DORA includes principles of proportionality, there is a cost to the implementation of DORA for all entities, because there is a shared need for resilience across the financial system and any group is only as strong as the weakest link.

The Chair commented that proportionality and compliance costs are critical considerations. DORA aims to balance resilience and avoiding excessive regulatory burden. Its ecosystem approach is grounded in outcome-focused collaboration.

3.4 Improving recovery planning

A central bank official noted that DORA will improve the prevention of and protection against cyber-risks, for example by establishing threat-led penetration tests as mandatory for significant financial entities in the EU. In Denmark threat intelligence-based ethical red teaming (TIBER) tests have been conducted since 2018 building on a framework developed by the European Central Bank (ECB). However, further work is needed on recovery planning. Improvement is required at the individual institution level and across the financial sector as a whole. Central banks are currently evaluating whether public back-up systems or offline transaction mechanisms should be established in case a bank is unable to operate for several days.

The Chair remarked that the expansion of threat-led penetration testing under DORA presents not only a valuable opportunity but also a challenge for supervisors. TIBER was originally designed by the ECB as a cooperative model between banks and supervisors, but there is now a

risk that it will become a traditional supervisory tool. Supervisors will need to adapt their approach and remain open to cooperation to maintain its collaborative nature.

4. Emerging risks and new measures needed

4.1 Emerging and evolving cyber-risks

A central bank official commented that the growing threat landscape, intensified by geopolitical tensions such as the war in Ukraine, has further underlined the urgency of tackling cyber-risks. A rise in incidents, notably distributed denial-of-service (DDoS) attacks, has led to heightened concern about the possibility of more severe disruptions. The 2022 invasion of Ukraine was a turning point that led to broader consideration of cyber and operational resilience in the financial sector. New areas of concern are now being discussed, including vulnerabilities in submarine cable infrastructure, the illusion of redundancy when multiple providers rely on the same infrastructure and structural shifts in the tech industry. Europe's dependence on non-European ICT providers, including CSPs, is a major issue that raises questions of long-term contingency planning and digital sovereignty.

An official emphasised that, from a macroprudential standpoint, assessing the size and interconnection of ICT providers alone is not sufficient. It is equally important to consider ongoing developments within the tech industry to properly evaluate systemic risks posed by these providers. This includes examining the strategic resilience of dominant ICT providers and their ability to sustain investment efforts over time. The so-called 'magnificent seven', some of which may be designated as CTPPs in the EU, are currently undergoing significant changes in valuation. At the same time, non western competitors such as Deepseek are emerging, potentially disrupting the market by offering similar technologies at lower costs. This could reshape competitive dynamics in a significant way. Another concern is the possible dependence of financial institutions on non-EU providers subject to foreign jurisdictions that may be exposed to geopolitical sanctions. Such reliance increases the risk of service disruption. A clearer understanding of these evolving challenges is essential to grasp their broader implications for digital operational resilience. Regulatory authorities must proactively address these issues, rather than assume that they will be resolved naturally.

An industry representative observed that, while the number of cyber-attacks has remained stable, their variety and sophistication has increased. Ransomware remains the most prevalent threat, with 'ransomware as a service' becoming common, although its success is still limited. Other risks include DDoS attacks and disruption attacks to infrastructure such as electricity, internet and subsea cables.

4.2 New policy measures needed

An industry representative suggested that industry-level cooperation within and beyond the financial sector is the most effective tool to monitor and tackle emerging cyber-risks. In the Netherlands, chief information security officers (CISOs) from large corporates, including financial and non-financial firms, have established joint communities to share intelligence and improve preparedness.

An official acknowledged the efforts of public institutions to build readiness. Stress testing and scenario analysis are increasingly common, with the ECB and several member states, including Denmark, taking the lead. There are also ongoing collaborations with the Bank of England. A new coordination body, the pan-European Systemic Cyber Incident Coordination Framework (EU-SCICF), has been established with the ESAs to enhance preparedness for systemic cyber incidents. There is a question of whether there is "bias to inaction", meaning a tendency to delay hard decisions or ignore emerging risks, in this area. Using analogies from the Apollo 13 mission, where action was taken promptly, and the Titanic, where the opposite occurred, the speaker argued that effective crisis response requires early acknowledgment of problems and the courage to act swiftly.

The Chair observed that DORA aims to generate momentum and fast responses. Incident reporting is now operational and continuously shared across Europe, with 24/7 points of contact established in member states, and coordination during emerging events is improving. The implementation of the EU-SCICF framework should help to counteract potential inaction by embedding a more proactive, systemic approach to operational resilience.

An official commended the work conducted by the ESAs in this regard in parallel with the implementation of DORA

4.3 The role of technology

The Chair observed that there is a tension between the tendency of rapidly evolving technologies such as distributed ledger technology (DLT) and AI to expand the threat surface and their ability to offer potential solutions to cyber-risks.

An industry representative highlighted AI's dual role in digital operational resilience, presenting both opportunities and challenges. On the one hand, AI enhances operational efficiency, customer experience and data analysis for faster decision-making. On the other, it is increasingly exploited by malicious actors to better target and sophisticate attacks. Regulators must balance the benefits and risks when shaping policies for AI and other technologies.

CSPs can play an important role in mitigating cyberthreats, in terms of both frequency and sophistication, and enhancing cyber-resilience. CSPs such as Google Cloud contribute to building resilience by continuously investing in security and developing the cloud infrastructure based in the EU. Partnerships are being developed with European financial institutions to offer services tailored to their specific workloads and data with strong sovereignty protections. The objective is to enable financial institutions to continue operations independently, even in the unlikely event of Google Cloud exiting the market.