Cyber and digital operational resilience

1. First lessons from the implementation of DORA

1.1 Overall added value of DORA

An official emphasised that one of DORA's main added values lies in its broad incident reporting and operational risk management approach, which improves the detection of operational and ICT disruptions within financial institutions beyond cyber incidents alone. Given that 38% of major incidents reported by banks relate to IT change, and as banks modernise ICT infrastructure and adopt new technologies, stronger processes and controls are needed to reduce unplanned network downtime. Cyber resilience stress tests have also helped bank management teams better understand cyber risks and strengthen governance structures, although improving board-level cyber expertise remains an ongoing process. DORA requirements have also helped codify supervisory practices that the ECB had already developed over many years, as operational and cyber resilience had long been a key supervisory priority.

Another official considered that DORA provides a solid framework that supervisors can build on in an uncertain geopolitical environment where operational resilience will remain a major risk driver. Although Latvia already had national rules on ICT risk and business continuity before DORA, the regulation represents a further step in risk mitigation by introducing a more structured market-wide approach. Larger institutions already have relatively mature governance and risk management frameworks, but DORA's main impact is on non-bank institutions and less mature firms, for which it has introduced a more targeted approach to risk management. The Latvian supervisor has invested significant effort in helping firms establish adequate risk management, incident reporting and third-party provider frameworks, moving beyond contractual arrangements towards clearer accountability across management layers.

An industry speaker stated that DORA, together with NIS2, helps establish appropriate resilience standards across the financial sector in a context where geopolitical tensions and the digitalisation of processes are significantly expanding the threat landscape. DORA has already improved incident reporting and governance and is proving useful, although market players remain on a learning curve. Its decisive test will come when the industry faces a major incident and the robustness of the framework can be assessed in practice.

1.2 Developing a resilience mindset throughout financial institutions

An official stressed that DORA should not be approached as a tick-the-box exercise, as the focus must remain on the broader objective of strengthening cyber and operational resilience. Compliance with the regulation is necessary, but not sufficient on its own to ensure resilience.

An industry speaker agreed that resilience must not become a purely tick-the-box exercise. DORA is a useful framework that can help reinforce resilience as a mindset. A risk-based approach to the application of DORA is important to ensure that all players adopt the right mindset and that the framework can adapt to evolving risks within different environments.

A public representative concurred that ensuring resilience requires the development of an appropriate mindset across all layers of financial institutions and management, rather than a purely compliance-driven approach. Resilience has become a key priority in discussions at the European political level. Another major priority shaping current discussions is the need to strengthen Europe's competitiveness, notably through regulatory simplification. The Digital Omnibus Package supports this objective, and streamlining reporting requirements including regarding cyber-risk is welcome because financial institutions often report the same cyber incidents to several authorities in slightly different formats, creating duplication without necessarily improving security. However, simplification should not lead to deregulation or lower standards, particularly in the current geopolitical environment and given existing resilience challenges. While some regulatory burdens may require simplification, resilience standards should not be weakened.

1.3 The role of threat lead penetration testing (TLPT)

An official noted that TLPT was previously conducted on a voluntary basis, but has now become mandatory under DORA every three years for certain banks. These tests are expected to provide important lessons on how banks can strengthen their resilience strategies. Around 80 banking groups have already been notified of the requirement to conduct tests, and the ECB has published guidance on TLPT implementation.

Another official explained that Denmark's public-private partnership on operational resilience, established in 2016 includes threat intelligence-based ethical red-teaming (TIBER) tests conducted voluntarily by financial institutions since 2019. The introduction of mandatory TLPT under DORA is therefore a welcome development. The use of ethical hackers in live production environments provides insights that traditional testing cannot deliver. One of the main objectives of TIBER testing is learning, which makes participation important. The findings and experience generated by these tests help senior management better understand what is at stake and what actions are needed to improve cyber-resilience. These tests have contributed to improving cyber resilience at technical, organisational and strategic levels across the financial sector. Based on this experience, extending TLPT to other critical sectors could also be beneficial.

An industry speaker stressed that TLPT exercises are not only about identifying and preventing vulnerabilities, but

also about developing the right mindset and the capacity to react and recover effectively. Operational resilience therefore requires frequent drills including senior management and should go beyond a purely theoretical or compliance-oriented exercise.

2. Progress in CTPP oversight and potential dependency risks

2.1 Implementation of CTPP oversight

An industry speaker observed that DORA had moved from policy debate to operational reality. The designation as Critical Third Party Players (CTPP) recognises the systemic importance of the services provided by these providers, while also representing a significant shift by bringing them for the first time under direct and continuous ICT risk oversight by the European Supervisory Authorities (ESAs). This new oversight approach is an opportunity to strengthen trust and transparency across the financial services ecosystem. Their firm, a major cloud service provider, had anticipated its designation as a CTPP and prepared for DORA over several years, making the transition more evolutionary than revolutionary. Cybersecurity and resilience were already embedded across its infrastructure, from subsea cables and chips to data centres, applications and customer platforms, supported by extensive audits conducted before DORA entered into force. Their firm also ensured that its control framework was aligned with both the spirit and the letter of DORA and supported customers in implementation, including by the early roll out DORA contractual terms in 2024.

The industry speaker added that engagement with the oversight team has been constructive and supported by clear guidance. While the implementation of the DORA oversight framework for CTPPs remains at an early stage, initial experience has been positive. The priority for 2026 is to build a collaborative relationship with the joint examination team and help supervisors develop a strong understanding of hyperscale technology, infrastructure, operations and control frameworks. Three conditions are important for effective CTPP oversight: an outcome-based approach focused on resilience outcomes rather than prescribing specific measures or methodologies; proportionality, given the differences among providers and financial institutions in terms of operational models, technologies used and risk environments; and consistency between European and national levels to ensure harmonised interpretation and application of the framework.

Another industry speaker noted that third-party risk remains challenging to manage and may require greater standardisation to help providers implement requirements more effectively.

2.2 Potential dependency and sovereignty risks

An official observed that dependence on non-EU third-party service providers emerged clearly as a risk during the implementation of DORA and the mapping of critical providers. Many of these dependencies are outside the EU, which raises additional resilience concerns in a context of heightened geopolitical tensions and increasing cyber and hybrid threats. In an increasingly digitalised society, cyber and operational resilience should be treated as a national security issue. The mapping, testing and structured approach required by DORA provides a clearer understanding of the actions needed to strengthen resilience across these different dependencies. Authorities and firms must ensure that the current digital infrastructure can continue functioning, even in crisis scenarios. In this respect, DORA provides a useful toolkit for raising awareness of risks and planning future action.

A public representative suggested that Europe should develop European alternatives to existing non-EU digital infrastructures and services in order to reduce dependencies. Resilience planning requires considering a broad range of scenarios, including the possibility of the United States becoming a less reliable partner and using systems supplied by US providers as part of sanctions or retaliatory measures. In some extreme scenarios, Europe's dependence on US technology infrastructure and services could become a major vulnerability. European alternatives should therefore be developed across all levels of the technology stack to ensure that Europe remains resilient across different geopolitical scenarios. This requires investment in European infrastructure, supported by appropriate regulation, European-level initiatives and political leadership.

An industry speaker stressed that hardware dependencies should also be part of discussions on resilience and strategic autonomy, as many hardware manufacturers are located outside Europe, creating an additional area of dependency.

Another industry speaker responded that their firm, as a major US technology provider, is committed to delivering best-in-class secure and resilient technology, while supporting European rules and sovereignty objectives. Both the technology itself and the way it is delivered are important. Their firm has worked on sovereignty issues for several years and developed technological responses structured around three pillars. The first concerns data sovereignty, allowing customers to control both data location and access, including through encryption keys stored outside the firm's infrastructure. The second concerns operational sovereignty, through arrangements enabling cloud operations to be handled by local partners within trusted European jurisdictions. The third concerns software sovereignty and portability, notably through open technologies supporting credible exit strategies, including the possibility to move services to another provider or back on-premises.

3. Evolving risk landscape and regulatory and supervisory implications

3.1 Evolution of cyber and digital operational risks in an increasingly digitalised society

An official stressed that the risk landscape has become more complex due to digitalisation and heightened

geopolitical tensions, some of which have already materialised. Although the financial sector has not yet experienced a major cyber-attack, the level of attacks has increased. Hybrid threats, including physical damage and broken cables, must also be taken seriously. Banks need to maintain ICT continuity, establish response plans in case of disruptions and integrate such scenarios into their resilience planning.

The official added that disinformation and social media dynamics are becoming increasingly relevant for financial stability and should therefore also be considered as part of operational resilience, even if these issues are not directly linked to DORA. Information flows through social media may affect the banking sector notably through misinformation campaigns. Banks therefore need communication plans and clear strategies in place, including to determine whether intervention is necessary. Supervisors are already discussing these issues with banks.

Another official agreed that supervisors and the financial industry need to monitor social media developments carefully, referring to the example of the Silicon Valley Bank run in the US, which was amplified by social media. Lessons should be drawn from this example in Europe, notably regarding liquidity management and the possibility that social media dynamics could trigger broader operational risks.

An industry speaker also noted that geopolitical tensions are a major concern for the banking sector, because the expanding threat landscape is intersecting with increasingly digitalised processes.

3.2 Sector-wide resilience and supervisory implications

An official explained that contingency planning work conducted in Denmark over recent years has been driven by a significantly deteriorated threat landscape requiring preparation for plausible extreme scenarios. While DORA strengthens resilience at individual institution level, it does not by itself guarantee continuity of critical financial services at the sector level. There is therefore a need to assess the financial infrastructure as a whole in order to identify single points of failure and determine how critical services can be maintained if a key infrastructure or institution is no longer functioning. This represents a significant undertaking and has required extensive cooperation across the industry including banks, other financial institutions and financial market infrastructures.

The official added that the recommendations resulting from the Danish contingency planning exercise, published in December 2025, highlighted the need for additional safety nets to ensure continuity of critical functions under extreme scenarios, with measures differing to some extent across market participants. The implementation of the measures required will be coordinated by the public authorities through dialogue with the relevant market participants. Further work may also be needed, including coordinated scenario exercises across the financial sector. Given the interdependencies involved, closer cooperation with sectors such as telecommunications and energy may also become necessary, together with more targeted requirements for services that are most critical for the financial sector.

Another official raised a broader institutional question regarding the growing number of actors involved in cyber oversight and supervision, including national competent authorities, the ESAs, national cyber authorities and ENISA. This multiplicity of actors could create inefficiencies in supervision, as previously observed in prudential and AML supervision. AML supervision could not be ensured effectively at the national level and had to be centralised, while earlier, prudential supervision had taken a similar path. A question therefore is whether cyber supervision may eventually also require an EU level centralised structure in the future.

4. AI implications for cyber and digital operational resilience

Referring to a study on AI adoption in financial services, the Chair noted that most AI applications currently being tested by financial institutions remain focused on internal operations and processes rather than customer-facing use cases, while the use of third-party providers to develop and deploy AI solutions is increasing.

An industry speaker emphasised that AI is playing an increasingly important role in the cyber threat landscape with malicious actors using AI extensively. A recent report showed that 44% of initial incidents result from the exploitation of third-party software vulnerabilities, increasingly automated through AI tools used to scan and exploit vulnerabilities. Attack timelines are also shrinking significantly, with attacks that previously took weeks to prepare now being executed within days. Financial institutions therefore need to use AI to address AI-related risks through agentic security operations combining detection, response and remediation, as speed has become a critical factor in cybersecurity.

In this context, the industry speaker explained that their firm is using advanced AI agents for detection, response and threat intelligence across billions of events, as this scale can only be managed effectively through AI-enabled systems. A "shared fate" model is used that goes beyond traditional shared responsibility approaches, aligning the provider's incentives and operational responsibility more closely with customer outcomes. The approach aims to combine resilience and security with customer control over data and critical operations, while ensuring operational portability through multi-cloud arrangements and credible exit strategies. This includes secure-by-default product configurations, guidance to customers on secure deployment and extensive sharing of insights and best practices through European and global industry channels such as FS-ISAC (Financial Services Information Sharing and Analysis Center). In some cases, direct technical and legal actions are also taken against cybercriminal activities, illustrated by the disruption of a large proxy network used by criminals to hide behind residential internet connections to conduct cyber attacks.

Another industry speaker observed that while AI brings important benefits in terms of efficiency and customer

experience, it also creates potential operational and security risks that must be actively managed. Their enterprise has established a dedicated competence centre for AI security and risks. Agentic AI is a particular challenge, as organisations may soon operate large numbers of autonomous agents whose activities need to be properly monitored and controlled. This requires inventories of deployed agents together with monitoring capabilities able to detect suspicious behaviour.

An official agreed that AI can support risk monitoring and mitigation, while noting that attackers are also increasingly using AI themselves. Institutions therefore need to assess AI from both defensive and offensive perspectives.

Wrap up

The Chair noted broad support throughout the discussion for DORA. DORA should be viewed as an operational framework rather than a tick-the-box exercise, supporting larger institutions already dealing with these issues while also providing a framework for smaller players and non-bank financial institutions to strengthen their cyber and operational resilience approaches. Public-private cooperation and mutual learning are important elements for strengthening operational resilience, notably through the exchange of concrete measures and experiences developed across countries at infrastructure and financial services level, including contingency planning and operational resilience initiatives. Given the common challenges faced across jurisdictions, greater attention should be paid to lessons learned and practices developed in other countries.

Beyond the ongoing implementation of the DORA CTPP oversight regime, the discussion also highlighted the importance of addressing third-party dependencies related to third-country providers notably of cloud services and AI. Questions around sovereignty have evolved significantly over time, shifting from questions regarding the physical location of critical registries and data towards broader issues surrounding the location and control of cloud infrastructure, data sovereignty and control over data access. Misinformation and social media dynamics are also important issues to consider, including their possible effects on financial sector performance and bank runs, alongside broader questions regarding the organisation of cyber supervision, which would require a broader political debate.