# Cyber-resilience: first lessons from DORA and emerging priorities

## 1. Implementing DORA: first lessons learned

### 1.1 Rationale and objectives of DORA

The chair opened the discussion by underlining the importance of the Digital Operational Resilience Act (DORA), the EU's comprehensive policy response to growing cyber and ICT risks in an increasingly digital and interconnected financial system. While digitalisation drives innovation and efficiency, it also increases the sector's exposure to operational disruptions and cyber threats.

Several key features characterise DORA: a cross-sectoral scope, an ecosystem-based approach, and a focus on outcomes rather than prescriptive rules, underpinned by a principle of proportionality consistent with the EU's simplification agenda. At the firm level, it requires institutions to strengthen their operational-resilience frameworks. At the system level, it enhances incident reporting, intelligence sharing, and advanced testing, and establishes a new oversight regime for critical third-party providers (CTPPs).

Designed to be future-oriented and technology-neutral, DORA is intended to adapt to evolving innovations such as cloud computing, encryption, AI, tokenisation, and DLT. With the regulation now in force, the chair emphasised that the key challenge is to translate its principles into effective implementation across the financial ecosystem.

### 1.2 Added value and conditions for success

A regulator welcomed DORA as a major step towards harmonised cybersecurity standards and a framework that empowers authorities to enforce requirements on third-party ICT service providers to which critical functions are outsourced. The benefits for essential services such as payments and cash operations are substantial. Although the regulation can be demanding for smaller entities, its proportionality rules help ease the burden.

Drawing on Estonia's long experience with large-scale cyberattacks, the country had already built a strong national cyber-resilience framework and established a dedicated cybersecurity agency alongside financial supervision. Yet, the increasing dependence of financial institutions on foreign ICT providers and the unpreparedness of many ICT providers for sophisticated attacks exposed the limits of purely national measures. DORA's added value lies in establishing consistent European standards and enabling cross-border enforcement of resilience obligations.

The regulator also stressed the need for a coordinated response between European and national financial authorities and cybersecurity agencies, ensuring they can act swiftly and cohesively when disruptions occur. This importance was illustrated, for example, by cyberattacks on major payment-service providers. Effective crisis management also depends on clear procedures, well-defined responsibilities, and specialised technical teams capable of intervening directly when financial services are affected.

At the Nordic-Baltic level, supervisors, central banks, and cyber agencies have already conducted joint cyber-resilience exercises, though these have mostly been led by US partners. The regulator encouraged the EU to take greater ownership in organising such cross-border drills, seeing DORA as a catalyst for stronger EU-wide cooperation and preparedness for large-scale cyber incidents.

An industry representative highlighted three positive changes introduced by the DORA framework in the banking sector.

First, DORA recognises that zero risk is unattainable, making recovery and continuity central to operational-resilience planning alongside prevention and mitigation.

Second, it integrates cyber risk into the broader ICT-risk framework rather than treating it as a separate category, prompting firms to clarify and coordinate internal responsibilities for risk management, reporting, and oversight, since no single individual can manage all these dimensions.

Third, it broadens the scope of oversight to encompass the entire digital ecosystem, reflecting the growing significance of outsourcing and third-party dependencies. Data from BaFin indicate that about two-thirds of payment incidents in 2024 originated from service providers rather than banks themselves, underscoring the need for this ecosystem-wide approach.

However, the industry representative noted that differences in authorities, rules, and implementation practices across member states still complicate coordination efforts and highlight the need for greater harmonisation to ensure consistent resilience across the Union.

Another industry representative observed that DORA has acted as a catalyst for progress among ICT service providers. The framework prompted many to conduct detailed internal gap analyses to identify shortcomings, implement corrective measures, and assess the speed at which compliance could be achieved. This levelling-up process has helped raise operational-resilience standards across the wider digital-financial ecosystem.

### 1.3 First experiences with the implementation of the CTPP oversight framework

An industry speaker explained that while existing financial regulations already impose outsourcing requirements on financial institutions, DORA goes further by introducing direct obligations for third-party ICT service providers. These include testing requirements and, for CTPPs, a system of direct supervisory oversight. This represents a major change in accountability, reshaping the relationship between financial institutions and their external suppliers.

The transition to this new regime is requiring significant educational and collaborative efforts, particularly with providers unfamiliar with a regulated environment. To facilitate implementation, the European Cloud User Coalition (ECUC) developed a compliance checklist for providers and maintained close dialogue with supervisors, underscoring the importance of a resilience approach encompassing the entire financial ecosystem.

Responding to a question from the chair on how CTPPs are supporting clients in implementing DORA, another industry speaker described how the regulation has prompted extensive engagement between their firm, a major cloud service provider (CSP), and its financial-sector clients, whose levels of preparedness vary widely. Helping clients interpret and apply DORA is indeed part of a CSP's role, guiding them through the operational and contractual implications of the regulation.

To that end, in early 2024, their firm updated its contractual agreements to align with the Level 1 DORA text and the forthcoming Regulatory Technical Standards (RTS) on outsourcing, ensuring that the core provisions of Article 30 are reflected in every contract[1]. A mapping exercise was also undertaken to link the firm's services and internal controls to DORA's requirements, enabling clients to understand how compliance is embedded in its processes. Guides and templates were also produced to help financial institutions maintain their registers of information as well as details on how subcontractors are selected and managed, thereby improving transparency across the entire third-party chain.

The industry speaker added that, going forward, CSPs will likely play a more active role in threat-led penetration testing and resilience exercises, depending on the criticality of the data and workloads hosted on their platforms.

The chair observed that DORA is designed to promote continuous improvement in cyber-resilience across the financial ecosystem, rather than imposing a fixed compliance deadline. The industry speaker agreed, but noted that some less-mature financial firms still attempt to shift the compliance burden entirely to CSPs, expecting them to guarantee adherence on their behalf. While CSPs can be key partners, ultimate accountability remains with the financial entity itself. The chair concluded that the success of DORA will depend on how financial institutions and service providers evolve together, striking a balance between shared responsibility and clear lines of accountability to build robust, system-wide resilience.

## 2. The UK's approach and progress in international coordination

An official explained that although the UK's operational-resilience framework is structured differently, it largely mirrors DORA's objectives. The UK has developed a comprehensive regime that combines policies on operational resilience, outsourcing, and third-party providers. A key distinction is that the UK oversight regime extends beyond ICT services to include any third-party function considered critical to financial market infrastructures (FMIs).

Scenario testing plays a central role in this framework. UK firms are required to design exercises based on "extreme but plausible" events, ensuring they are substantive rather than compliance-driven and involve all relevant stakeholders to make them holistic and realistic. As threat actors become more sophisticated, incidents once considered extreme, such as state-sponsored attacks, are now part of the regular threat landscape, underscoring the need for continuous adaptation. The Bank of England plans to issue new cyber-resilience guidance later in the year, focusing on FMIs. The guidance will summarise recent lessons, identify services most critical for financial stability, and clarify the capabilities required to mitigate systemic risks.

Global consistency is also improving, particularly in incident and outsourcing reporting, supported by the FSB's FIRE framework, which promotes cross-border alignment and a shared understanding of third-party dependencies. This approach helps identify critical providers across jurisdictions and facilitates learning from incidents in other markets.

Because critical service providers operate globally, disruptions can cascade rapidly across markets and borders. The global IT outage caused by CrowdStrike in July 2024 illustrated how quickly such incidents can spread and underscored the need for coordinated responses across jurisdictions and active information-sharing. The UK framework promotes this through industry-wide stress-testing exercises, such as SIMEX[2] and sector-specific tests like CCP fire drills, which strengthen collective preparedness and promote learning across the ecosystem.

In response to a question from the chair about improving communication and coordination among authorities during cross-border incidents, the official confirmed that international collaboration has strengthened and reporting frameworks have become more consistent. Nonetheless, further work is needed to achieve a common understanding

1. Article 30 defines the mandatory contractual elements between financial institutions and ICT third-party providers, such as service-level terms, access and audit rights, and incident-reporting obligations.
2. SIMEX (Systemic Incident Management Exercise) is a large-scale simulation led by the Bank of England to test the financial sector's collective response to severe operational or cyber incidents

of threats, harmonised response measures, and a clear division of responsibilities between jurisdictions.

## 3. Emerging risks and technological responses

### 3.1 The evolving cyber-risk landscape and policy implications

An official noted that the cyber-risk environment is becoming increasingly complex and sophisticated, as technological innovation brings both new vulnerabilities and new means to counter them. A key challenge is to manage this balance effectively, ensuring that innovation enhances rather than undermines resilience.

To address this evolving landscape, digital-resilience regulation must remain outcome-based and technology-neutral. Moving from legacy systems to cloud-based infrastructures can help build resilience by design, but also introduces concentration risks and a new risk profile compared to in-house systems, which requires robust shared-accountability models, clear playbooks, and tested controls, alongside potential oversight of the most critical third-party providers.

An industry representative considered that challenges to operational resilience are evolving rather than fundamentally changing. Social engineering remains the dominant threat, but attack methods are increasingly sophisticated, using deepfakes, synthetic voices, and mixed online/offline vectors, such as postal letters containing fraudulent QR codes and the scale of attacks is increasing. The rise of "cybercrime-as-a-service" is also helping to industrialise such attacks, lowering the technical threshold for entry.

Hybrid threats, where disinformation on social media and instant payments can amplify and accelerate financial shocks, are also emerging. The Silicon Valley Bank episode, with 85% of deposits withdrawn in 48 hours, illustrates the speed and communication dimensions of modern crises. In such a context, stakeholders must have a clear understanding of their respective roles and of how existing frameworks - DORA, the Digital Services Act, and national regimes - interlock to maintain confidence and stability.

Another industry representative explained that their firm applies a defence-in-depth approach, a multi-layered security architecture, since no single control can counter all potential attack vectors. This architecture now integrates AI tools to enhance threat detection and response capabilities.

### 3.2 The dual role of technology: new risks and new solutions

Several panellists agreed that technology, particularly AI, creates both new risks and new defences for operational resilience, equipping both sides with ever more sophisticated tools.

An industry speaker described the dual role of AI. On the attack side, AI enables more precise and scalable threats, such as targeted phishing campaigns, deepfakes, accelerated malware generation, and large-scale disinformation. On the defence side, AI can enhance detection, response, and incident-handling capacities, helping security teams cope with expanding attack surfaces and data volumes. However, it is not a silver bullet and cannot replace analysts, security teams, or the human oversight that remains central to decision-making. In addition, firms deploying AI must do so securely and consistently with their risk and security policies, recognising that AI systems carry their own risks and vulnerabilities.

An official added that while advanced AI improves fraud detection and surveillance, its black-box nature poses governance and supervisory challenges, increasing unpredictability under stress and complicating regulatory intervention. The growing concentration of AI providers may also create single points of failure.

The chair agreed that technology brings both solutions and vulnerabilities, describing it as an "ever-evolving race" rather than a winnable war. A positive development, is that resilience is increasingly built into system design. The chair also underlined the financial sector's natural affinity for AI, given its longstanding use of data models, and emphasised that human judgment and oversight are indispensable to make AI effective in practice.

The official noted that even defensive technologies, such as faster detection and recovery systems, can be weaponised by attackers. In a 24/7 financial system, incidents can escalate within minutes, underscoring the importance of joint playbooks, coordinated testing, and collective preparedness across the financial ecosystem. Tokenisation also brings new challenges and opportunities for cyber resilience[3]. The layered smart contracts and blockchain protocols used to process tokenised transactions increase complexity and can obscure market dynamics, potentially heightening operational fragility. At the same time, these technologies can strengthen oversight. For example, in the case of stablecoins, they can be used to monitor issuance directly on-chain. The Bank of England's Project Pyxtrial aims to track issuance in near real time and flag deviations, contributing to enhanced transparency and stability.

## 4. Digital assets: specific operational challenges and regulatory adaptations

An industry speaker explained that for ICT service providers supporting Crypto-Asset Service Providers (CASPs), implementing DORA has been a complex

3. Tokenisation also creates new opportunities and challenges from an operational perspective. While it can improve clearing and settlement efficiency, it may also create liquidity inefficiencies due to the pre-funding required for atomic settlement. There are also mismatch risks between on-chain "digital twins" and the underlying real-world assets they represent, which must be carefully monitored.

exercise requiring close collaboration among stakeholders. Many CASPs previously operated outside any regulatory perimeter before the introduction of MiCA, and concepts such as KYC and anti-terrorist financing were initially unfamiliar. Over time, however, these entities have adopted risk-management standards comparable to those of traditional finance, significantly strengthening the sector's maturity and resilience.

The preparation process for DORA has revealed areas where the framework could be refined to better address the specific risks of digital-asset activities. This includes the need for greater technical precision to prevent certain incidents such as those seen on some crypto-asset platforms, for instance by discouraging the use of blind-signed hardware security modules or other insecure key-management technologies. The key challenge is to balance DORA's flexibility and adaptability with the degree of specificity required to manage risks in this rapidly evolving environment.

Building on this, the speaker suggested that DORA could inspire a broader reconsideration of how regulation applies to custodial and software services, ensuring that frameworks evolve to address the distinct characteristics and risks of digital assets while keeping pace with technological innovation.

Asked whether the digital-asset sector requires further regulation given its growing importance, the speaker supported the idea of a digital-asset- or custody-focused extension of DORA. The first step, however, is to define what a good regulatory outcome looks like in a technology-neutral manner. Many supervisors still associate sound security with offline storage in a vault, a model that fails to reflect the true nature of digital assets, whose utility lies in being in motion within blockchain networks, operating without intermediaries and secured through cryptographic control rather than traditional safekeeping. Regulation should therefore ensure that digital assets remain secure while accessible and transactable, recognising this distinctive custody model.

The chair acknowledged the need to adapt custody concepts to the specificities of digital assets and agreed that existing frameworks such as MiCA and DORA provide a solid basis on which to build further regulatory progress. A pragmatic, evolutionary approach indeed offers the best way to strengthen outcomes while allowing for targeted adjustments as technologies and markets continue to evolve.