# CYBER RESILIENCE IN THE AI ERA

KERSTIN PILT

Chair of the Management Board – Estonian Financial Supervision Authority (Finantsinspektsioon)

## DORA delivers real results in Estonia — But the harder work begins now

DORA is already delivering real resilience benefits in Estonia and across the wider Baltic region. Its biggest contribution has been turning supervisory expectations into enforceable legal obligations. Much of what DORA now requires; ICT risk management, incident reporting, testing, third-party oversight, was already supervised in Estonia before DORA came into force, based on EBA guidelines and other soft-law tools. What has changed is the legal footing: we now have a clear, directly applicable basis to enforce these requirements. As a result, management bodies at DORA-regulated firms are paying closer attention to operational resilience, ICT risk governance has improved, and oversight of critical third-party dependencies has become more structured. In a region where cyberattacks are a constant threat, driven in large part by a hostile neighbor, and where our societies are highly digitalized, this shift is not a mere technicality. It closes the gap between best practice and legal obligation.

The harder work lies ahead: operationalizing the Critical Third-Party Provider oversight framework. Overseeing providers whose services underpin the resilience of the European financial system requires close coordination between Lead Overseers, national authorities and the providers themselves, many of which sit outside the EU and outside supervisors' traditional reach. Given how concentrated the market for some of these services already is, getting this right is not optional: it is foundational to system-wide resilience. Three open questions will decide whether this becomes effective rather than a paper exercise: do Lead Overseers apply consistent methodologies across Member States; are escalation paths fast enough; and do providers whose regulatory ties have traditionally lain elsewhere take the framework seriously? This is a multi-year effort, and success will be judged less by initial designations than by how the first disputes are handled.

**Resilience will be judged not by standards adopted, but by how consistently we apply them.**

There is a further complication. Some third-party providers in Estonia: telecoms operators, digital identity and signature service providers, are critical to the financial system, yet their small size means they will never fall within scope of the oversight framework. This is not a hypothetical gap, it is a real one, since these are services most people use daily without thinking of them as part of the financial system. For them, we rely on national legislation and cooperation with other authorities holding the relevant mandate. Our priorities follow the regional threat picture. Cyber resilience remains, and will remain, the core mission, not a box we tick once DORA implementation is complete. AI, meanwhile, is becoming central to the resilience landscape creating real opportunities for cyber defense, anomaly detection and incident response, alongside with new dependencies, risks and attack vectors of its own. Even so, we do not see a need for a wholly new AI regulatory regime at this stage as DORA's framework is broad enough to absorb these. The priority now is consistent implementation, not more legislation. And implementation calls for real proportionality. Our market ranges from systemic banks to firms with two or three employees, all under the same regulation. An approach calibrated for the largest players will simply be unworkable, or ignored, by the smallest - proportionality is what keeps the framework credible across such a varied market.

Supervisory cooperation should be strengthened further; this is where the greatest gains are still to be made. DORA's requirements, and the threats behind them, are broadly shared across Europe, which makes cooperation a necessity, not a courtesy. Estonia has pursued this on several fronts: domestically with our Central Bank, the Police and Border Guard Board and Information System Authority; and internationally with peer supervisors. This June we hosted a joint training with the Bundesbank in Tallinn, informally known among participants as the "DORA on-site inspectors' festival," bringing inspectors together to align practical approaches. We would welcome common supervisory expectations, harmonized inspection methods, better threat-intelligence sharing, and closer alignment between Lead Overseers and national authorities. We understand that this does not happen automatically but requires sustained effort from supervisors on all sides. Ultimately, digital operational resilience will be determined not by the number of technical standards adopted, but by our ability to apply them consistently and respond together to an interconnected threat landscape.

SOFIA TOSCANO RICO
Deputy Director General – European Central Bank

# Safeguarding Europe's banks in the digital age

**A transformed risk landscape**

On 7 July 2026, the European Systemic Risk Board (ESRB) issued a warning[1] on systemic cyber risks stemming from frontier artificial intelligence (AI) models, acknowledging how these models are changing the cyber threat landscape for the EU financial system. On the same date, the European Central Bank (ECB) published a letter[2] to the CEOs of banks directly supervised by the ECB, framing AI-enabled cyber threats as a long-term shift in the threat environment and calling on banks to strengthen their information and communications technology (ICT) resilience.

Frontier AI models are highly capable AI models that represent the leading edge of current or anticipated technological development and mark a paradigm shift in cybersecurity as they can discover and exploit software vulnerabilities at unprecedented speed and scale. This has profound implications for the confidentiality, integrity and resilience of banks' ICT systems, particularly in the case of legacy systems.

Compounding this challenge is third-party risk. In many areas, including AI, EU banks are becoming increasingly reliant on a few external providers from outside the EU, exposing them to strategic dependency and geopolitical risks. Moreover, the same dependencies expose banks to the risk of cascading disruptions arising from cyber incidents, operational failures or outages, even when the banks themselves are not directly targeted.

**Keeping pace: supervision of ICT and cyber risk**

Regulation has advanced in parallel. The Digital Operational Resilience Act (DORA) was designed to ensure that financial entities within the EU can withstand, respond to and recover from ICT-related disruptions, while the AI Act sets harmonised rules to regulate AI systems based on their risk level. Alongside these legislative initiatives, and building on the role provided for in DORA, the European Supervisory Authorities, at the request of the ESRB, have established the pan-European Systemic Cyber Incident Coordination Framework (EU-SCICF) to strengthen coordination during systemic cyber incidents.

Monitoring the risk landscape carefully, the ECB has kept operational and IT resilience firmly and consistently in the focus of its banking supervision. One cornerstone was the cyber resilience stress test conducted in 2024, in which 109 banks faced a severe scenario disrupting core systems and had to demonstrate their response and recovery capabilities. As a complement to this, in 2023 and 2024 European banking supervision conducted cyber dry runs to test whether the ECB and national competent authorities were sufficiently prepared for system-wide cyber incidents affecting both the authorities and banks. The exercise was extended to other EU bodies, such as the European Banking Authority (EBA) and the Single Resolution Board (SRB), when it was repeated in 2026. Incident reporting also helps supervisors rapidly identify major cyber events and coordinate crisis responses when needed.

**Operational resilience comes down to preparedness: banks must be ready.**

To address third-party risks resulting from the use of cloud services, the ECB published its *Guide on outsourcing cloud services to cloud service providers in 2025*[3], encouraging geographically diversified data centres, clear exit strategies for outsourced cloud services and regular assessment of concentration risks.

**From compliance to culture: owning resilience**

These structural challenges cannot be tackled in isolation: in a system where the weakest link can affect many, sharing good practices and working together are essential. Banks have to be able to respond effectively to the transformed risk landscape. A bank's management body therefore needs a proper understanding of the evolution and materiality of such risks in order to take adequate and timely decisions to manage them.

But that is not all. Management boards must also champion a culture of resilience within banks, and executives must invest decisively in modernising legacy systems and hardening defences. Such investments are not mere operational costs; they will be the foundation of renewed competitiveness.

Ultimately, operational resilience comes down to preparedness: banks must be ready.

1. *https://www.esrb.europa.eu/news/pr/date/2026/html/esrb.pr260707~4e1b68241a.en.html*
2. *https://www.bankingsupervision.europa.eu/press/letterstobanks/shared/pdf/2026/ssm.2026_letter_on_AI_enabled_cybersecurity_threats.en.pdf*
3. *https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/ssm.pubcon240603_draftguide.en.pdf*

MOIRA CRONIN
Partner, Digital Risk & Resilience – PwC Ireland

# Cyber resilience after DORA: from compliance to capability

Financial services firms face a cyber-threat landscape evolving in speed, scale and consequence. Firms can no longer contend only with isolated attacks. They operate in an industrialised, interconnected and adaptive threat environment shaped by ransomware, identity compromise, supply-chain disruption, geopolitical activity etc. and AI-enabled social engineering, including deepfakes targeting executives and clients. The ECB's 2024 cyber resilience stress test confirmed that while banks can respond, recovery capabilities remain uneven.

The most significant shift is not volume but propagation. Impacts move rapidly across firms, third parties and markets. Heavy dependence on cloud services, software providers, managed services and outsourced operations delivers efficiency and innovation, but also concentration risk and complexity. A cyber incident or technology outage can quickly become a systemic operational resilience event, with direct implications for customers, counterparties, regulators and trust. The EU's Digital Operational Resilience Act (DORA) has sharpened governance, accountability and focus across a number of areas. The first phase of implementation, however, should be seen as the beginning of a more demanding resilience journey, not the end.

The areas where firms remain least prepared are increasingly clear.

**First,** end-to-end visibility: many firms understand applications and controls better than how critical services are actually delivered, and where true single points of failure sit, particularly across fourth and nth-party dependencies.

**Second,** exit and substitutability planning for critical ICT third-party providers under DORA Article 28 remains immature, especially where cloud or specialist providers have few viable alternatives.

**Third,** data resilience: immutable backups and validated recovery integrity still lag control-focused investment.

**Fourth,** operational effectiveness: firms must demonstrate they can respond to severe but plausible scenarios and meet DORA's tight incident reporting timelines under pressure.

**Fifth,** ownership and board challenge: cyber resilience cannot sit solely with the CISO or CIO — it requires business accountability, active board engagement and non-executives capable of meaningful challenge. Legacy technology, technical debt and cyber talent shortages compound each of these gaps.

> DORA sets the standard; resilience is the strength and stamina firms must show.

Investment has risen, but too much remains directed at compliance evidencing rather than capability building. Compliance asks whether the framework is in place; resilience asks whether critical services can continue when all else fails. Both matter, but they are not the same. The risk after DORA is that activity concentrates on evidence packs and regulatory deadlines, rather than firm-wide capability to withstand, adapt to and recover from disruption.

The next phase should be practical, prioritised and outcome led. Firms should focus on three priorities: validating critical services and their end-to-end dependencies, including concentration in cloud; strengthening resilience testing beyond discussion-based exercises and embedding resilience in strategic decisions on transformation, outsourcing and technology modernisation.

A Minimum Viable Company lens can help. Rather than treating everything as critical, this recent PwC campaign takes the approach to identify the services, processes, people, technology and third-party dependencies that must remain operational or be restored first. It creates clarity around recovery priorities, investment and board reporting, and focuses leadership on protecting what matters most to customers, regulators and markets.

Artificial intelligence will play an increasingly important role in cyber resilience. Used well, AI can improve detection, triage, threat intelligence, vulnerability prioritisation and incident response. Attackers are also adopting AI rapidly through deepfakes, automated reconnaissance and adaptive malware meaning defensive adoption is no longer optional. However, AI is not a substitute for resilience fundamentals. Its effectiveness depends on high-quality data, reliable telemetry, accurate asset inventories, robust governance and human oversight. Firms must manage risks associated with AI itself, including model security, data integrity, explainability, accountability, adversarial manipulation and concentration in foundation-model providers.

In high-impact decisions containment, recovery, customer communications, regulatory notification AI should augment expert judgement, not replace it.

DORA has provided a strong foundation. The challenge now is to convert it into demonstrable resilience across critical services, third-party dependencies and recovery capability. The firms that lead will treat DORA as a catalyst, not a ceiling. In an increasingly digital and interconnected financial system, cyber resilience is no longer only a regulatory obligation it is a strategic imperative, a trust differentiator and a driver of long-term competitiveness.

JESSICA KAFFRÉN
Member of the Management Board – J.P. Morgan SE

# Refining DORA in an era of frontier AI cyber risk

With a sector as interconnected and interdependent as financial services, it is impossible for any one entity to be resilient in isolation. The largest banks have long been subject to stringent ICT and cybersecurity risk management rules. But DORA has raised the level for the sector as a whole and given European financial entities a head start on the urgent work of cyber hygiene and IT risk management.

That said, DORA, like any ambitious first attempt at major regulation, is not perfect. Reforms to two areas in particular would materially help defenders without weakening regulatory standards.

**Incident reporting**

After more than a year in operation, it is clear that DORA incident reporting is capturing too many non-material incidents, creating strains on financial entities and supervisors alike. The wide and complex array of criteria and thresholds that dictate reporting under DORA are not good measures of how severe an incident actually is.

Two examples from the current reporting criteria help to illustrate the point. First, the geographic spread criteria indicates primarily that the firm has legal entities in different member states, not that an incident was significant. Second is the cost criteria. It belongs in a final report, as part of understanding an incident after the fact, not among the criteria that decide whether it is reportable in the first place. Business-as-usual response costs should be excluded outright, since they measure effort, not severity.

If DORA's incident reporting criteria can be properly recalibrated around severity the result will be less noise for authorities and less wasted effort for firms.

**Criticality**

The second area is criticality. The definition of critical or important function (CIF) is built for outsourcing, not for resilience. Every service should benefit from strong security and resilience. But if criticality is to be usable within a firm's resilience framework, it must be reserved for the smallest possible number of genuinely essential services. A definition that sweeps too broadly dilutes focus precisely where focus matters most.

> The fundamentals of cyber hygiene are more important than ever.

The tensions this creates are already showing. Some EU authorities have begun pushing the concept of a smaller subset of CIFs that require additional resilience, while others are de-facto broadening the interpretation of what is critical.

The EU needs a consistent concept of criticality focused only on the services most essential to the stability of the firm and the sector and which therefore require a degree of resilience beyond the already high standards of financial entities.

**AI**

Finally, AI. It is already reshaping the threat landscape. The window we once had to analyse and implement a security patch has shrunk to almost nothing: many models can now reverse-engineer a patch and build a working exploit in less than a day. Firms must radically accelerate their patching, but we should acknowledge that attackers will always have the speed advantage and we cannot rely on patching alone to mitigate the risk. That is why the fundamentals of cyber hygiene are more important than ever.

Earlier this year, we set out ten steps firms can and should be taking[1]. We focused on the fundamentals: reducing end-of-life dependencies, managing privileged access well, filtering outbound traffic from production systems. The overwhelming majority of cyber risk is still won or lost on these basics.

But it is not only financial entities that should be acting. The worsening threat landscape means authorities also need to consider what they can do to reduce risk exposure. In the U.S., the Federal Banking Agencies (FBAs) have recognised the essential role they play in keeping the sensitive data of financial entities safe. In their statement on the handling of highly sensitive information, the FBAs acknowledge that the collection and storage of certain information such as details of control weaknesses, network diagrams penetration test results or certain business data, should be minimised through options including accepting on-site review only or the collection of summarised or redacted versions of documents[2]. They also commit to notify firms of any material breach affecting their confidential supervisory information within 72 hours. These changes are not about lowering supervisory standards. Rather, they are about good security fundamentals of minimising data exposure to what is strictly necessary to properly supervise firms.

**Conclusion**

The task ahead is to build on DORA's positives. We need to keep our eyes on the fundamentals, to refine the rules where they create noise without improving risk management, and to confront honestly, but urgently, what frontier AI means for the cybersecurity risk faced by the sector.

1. *https://www.jpmorganchase.com/about/technology/blog/fortifying-the-enterprise-10-actions-to-take-now-for-ai-ready-cyber-resilienceç*
2. *https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20260716a1.pdf*

DEA MARKOVA
Policy Director
- Fireblocks

# Better organised threats deserve a better organised response

**Better organised threats**

Digital assets are becoming mainstream finance. In 2026, use cases have matured across cross-border settlement, bank and asset manager tokenization, and payment networks, driving significant volume. Stablecoin transaction volume reached a record $1.79 trillion in June 2026 alone[1], up 63% month over month. In July, the DTCC, which safeguards more than $114 trillion in securities, converted assets held at its depository into tokens and used them in live production trades with more than 30 firms, ahead of a full-service launch in October[2]. When the plumbing of US capital markets tokenises its own book, the asset class is no longer at the edge of the system.

As the sector matures, so do its attackers. Digital asset theft is no longer opportunistic. It is patient, well-funded, and increasingly industrialised. Hackers stole more than $3.4 billion[3] in digital assets in 2025, and over $17 billion since 2020. What changed through 2026 is organisation and sophistication.[4]

For instance, DPRK actors are running a sustained, parallel, multi-vector campaign, focusing on social engineering. Three confirmed DPRK-linked operations occurred in April 2026 alone, each targeting a different layer of the digital assets stack: those authorised to approve a protocol's decisions, the personal laptops of the engineers who build it, and the systems that confirm whether a transaction is genuine.

Nefarious actors spend months building trust with employees before they strike. Criminal networks sell ready-made attack kits to less skilled operators, enabling theft at scale by people who lack technical skill.

Tokenization changes the attack vectors for any tokenized assets, and thus requires dedicated risk management and rulemaking. For example, the so-called blind signing: attackers obtain valid signatures by manipulating signers into approving transactions whose content they do not fully understand. Blind signing has been a persistent attack vector across the industry, with examples including the WazirX[5] ($234M, July 2024) and Bybit[6] ($1.46B, February 2025) incidents.

**Leveraging AI for good & bad**

AI is now adopted on both sides of this fight. Its value to resilience depends entirely on where you let it act.

> As digital assets move into mainstream finance, threat actors have grown more organised and industrialised. AI can be an asset, on both sides of the fence. Europe's resilience rules need a dedicated focus on digital assets.

On offence, we have already seen what it does. Attackers used AI to fake identities and forge paperwork, thus taking control of a platform's website and sending users to a fraudulent copy. In another case, a criminal hid a payment instruction inside an ordinary-looking coded post on social media. An AI assistant passed it to a second AI system, which made the transfer automatically.

On defence, AI earns its place. It can scan software for weaknesses before release, spot unusual transaction patterns faster than any analyst, monitor third-party providers for emerging risk, and help staff catch deepfake voices and video used in scams. These are analysis and detection tasks.

**The gap post DORA**

The EU's Digital Operational Resilience Act has gone a long way to converge industry and its supervisors onto a higher cybersecurity standard. With the MiCA transition just finalised, it is too early to assess the outcomes of all EU crypto-asset service providers being subjected to DORA.

What we learned, as a third-party technology provider, is that the requirements on the custody function, stemming from MiCA, DORA, and the payments, capital markets, and AML rulebooks, leave a wide range of choices to industry and its supervisors. The requirement of an independent review of cryptography-related code is a good example. How and how often to audit one's third-party vendors is another.

A common supervisory action on CASPs' digital operational resilience for custody was launched eight days after the MiCA deadline, which we understand to reflect the same concerns.

The experience of securing digital assets is in short supply, in both crypto-native and traditional finance, and the absence of dedicated guidance opens the EU to implementation vulnerabilities.

Primary legislation and technical standards are, rightly, technology neutral. Yet safeguarding tokens, whether crypto, financial, or payment instruments, changes the operational resilience paradigm that applies.

The CSA is a helpful step. A dedicated report on the learnings, and guidelines, ought to come next. Better organised threats deserve a better organised response.

1. *Visa Onchain Analytics Dashboard (Allium Labs), June 2026, accessed August 2026.*
2. *DTCC press release, 15 July 2026.*
3. *Chainalysis, 18 December 2025.*
4. *Fireblocks Global Digital Asset Threat Report Q2 2026.*
5. *WazirX statement, 18 July 2024 (losses "exceeding $230 million").*
6. *Chainalysis, 18 December 2025.*