CYBER-RESILIENCE: FIRST LESSONS FROM DORA

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

DORA – a multifaceted approach to digital operational resilience

Digital operational resilience is a fundamental underpinning of a resilient and well-functioning financial system supporting the economy and serving the needs of citizens. Financial services are, at their core, about information and data. The threat surface is large, the risks are significant and increasing, and the potential impact is great.

The Digital Operational Resilience Act has been live for over six months. DORA represents significant ambition – to introduce a single, far-reaching framework of regulation that can be applied to every financial firm whatever their size, whatever their complexity, whatever their business model. This aspect, combined with the oversight regime for critical third party providers, as well as the focus that DORA places on fast information flows, makes it a true form of smart ecosystem regulation. In the same way as network effects bring further benefits the more initial benefits are achieved, something similar applies in the context of an ecosystem construct. The more we can achieve enhanced resilience across the ecosystem the more individual participants will benefit. The delivery of the suite of technical standards that provide DORA's implementation details completed by the three European Supervisory Authorities (ESAs) together with more than 40 national competent authorities (NCAs) 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, the ESAs and NCAs are focusing on convergence of supervisory approaches to implementation. This includes seeking to ensure that more than 40 national authorities implement DORA's harmonised cross-sector approach in a consistent, outcomes focused manner. This will not be an easy task, but good engagement and discussions continue at ESA and NCA level to ensure just that.

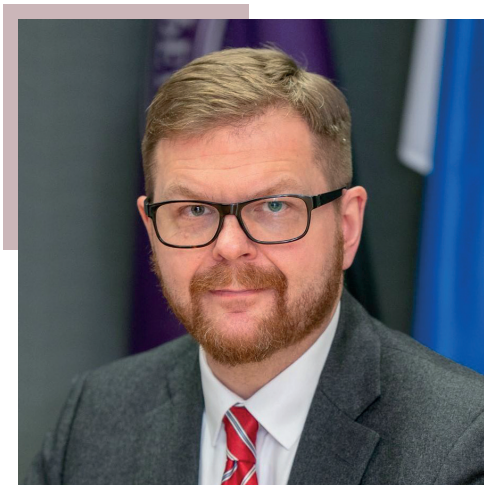
Information and Communication Technology (ICT)-related incident reporting has been underway since earlier this year. Incidents are now being reported across the Union as required and the ESAs as well as NCAs are monitoring and analysing these closely. This will over time transform knowledge, preparedness and responsiveness.

> **A single, far-reaching framework of regulation that can be applied to every financial firm.**

In April, financial regulated entities subject to DORA submitted the Register of Information of contractual ICT services provided by third-party providers and this forms 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 with an NCA's broader supervisory engagement plan for a given financial regulated entity. This of course means that financial entities will be assessed at different times, similar to supervisory engagements that address other safeguarding outcomes.

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

As we look to the future, the combination of data from ICT reported incidents, the analysis of the Register of Information for critical ICT suppliers and the now established supervision in line with DORA will further aid the operational resilience of ICT systems of financial firms. While operational resilience aims to build capabilities to deal with risk events when they materialise, operational risk management focuses on preventing those risks from happening in the first place. As a financial regulator, looking across the sectors that we supervise, both operational risk as well as operational resilience remain key areas of focus for us. This reflects the increasingly sophisticated digital environment and therefore the increasing importance for regulators to understand vulnerabilities and the potential for system wide disruption.



KILVAR KESSLER

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

Digital finance needs basic rules, vigilant oversight and close cooperation

Digital tools in finance and digital operational resilience have been central issues for financial supervision for at least a decade. The EU Digital Operational Resilience Act of 2022 (DORA) enhances cross-border operation and cooperation between authorities, and the EU AI Act of 2024 (AI Act) will harmonise how we address the risks from state-of-the-art technology. It is crucial that we pay close attention to the interplay between DORA and the national security frameworks of member states, and that we foster a business-friendly environment that can allow trial and error, and that does not stifle rapid technological advances such as artificial intelligence (AI).

People in Estonia rely widely on public digital solutions, and this has promoted simplicity and speed in interactions between citizens and the state. This has in turn provided an important foundation for the high level of digitalisation in financial services. The digitalisation of financial services has cut costs. However, opportunities also bring risks. The history of cyberattacks in Estonia began in 2007 when the banks and other institutions were massively attacked for the first time by foreign, state-related actors. Since then, Estonia has created the legal framework that is needed to address cyber threats and has learned how to deal with them.

The main challenge for businesses as they entered the DORA era was the volume and detail of regulatory requirements, and the delays in those requirements appearing. Here, proportionality provided some relief for smaller and less ICT-mature financial institutions. The challenge for the public sector at that juncture was to determine which authority would be responsible for implementing and supervising DORA, as Estonia already had the infrastructure needed in place within an emergency framework that came under national defence. After the various options had been carefully weighed, the financial supervisory authority took responsibility for DORA, but a framework for cooperation was set up with the Information System Authority, the agency responsible for cybersecurity in Estonia. However, it remains to be seen how the EU agencies, the member state agencies operating under the EU framework, and the member state agencies operating under national defence rules will cooperate in the event of an emergency. A first step that would help in overcoming potential issues could be to hold joint exercises, which the Nordic-Baltic region has been successfully doing for several years by now.

Outsourcing and concentration risk were among the drivers of the adoption of DORA. Since the act was passed, AI solutions have gained momentum. These are algorithms that use vast amounts of input data and combine it in a particular way. All the major banks in Estonia have an AI strategy in place now, and 37% of banks are actively using AI solutions, while 63% are piloting cases. AI is used in data analysis including credit scoring, cybersecurity, simple product selection, combating fraud, handling customer complaints. The banks expect to increase their AI use cases.

Even at the current phase of development, businesses see AI as broadly beneficial, citing operational efficiency, better decision-making, and more sophisticated client experiences. However, there are risks from using AI. Three main concern data protection and privacy; cybersecurity and the immaturity of the algorithms; and dependency on foreign AI. As AI use cases are still in their early stages, it is easier to mitigate the main risks today. Banks have risk management measures in place, but in the long run, maturity and dependency risks will be crucial and will probably have to be accepted to some extent.

The AI Act will gradually come into force between August 2025 and August 2027. The existing rules, including DORA, provide a good starting point for taking supervisory actions and initiatives to address AI-related risks now. At Finantsinspektsioon, a separate ICT risk supervisory area with its own department dedicated to it was established years ago to keep the topic in focus, as we predict that the importance of technological risks will in future be equal to or even surpass that of financial risks. In the long run, financial supervisors will need to be equally skilled in the three important areas of law, finance and ICT.

The interplay between the EU rules on cyber and relevant national security norms is crucial.

We are keeping a close focus on AI, and we are monitoring developments at least annually. This type of pulse check will guide our supervisory priorities. We are cautious but we tend to be open to increased use of AI in finance, and so we welcome the AI Act. However, there may come a need to slow or stop the legislative train, simplify the existing regulations, and place even more emphasis on creating a business environment where European AI can be born and can flourish.

SASHA MILLS
Executive Director for Financial Market Infrastructure – Bank of England

Ensuring a dynamic and adaptive approach for operational resilience

In today's interconnected and digitised financial landscape, operational resilience is a key priority for financial regulators. Whilst technological change unlocks powerful opportunities for innovation and efficiency, it also introduces fast-evolving cyber and operational threats. To navigate this challenge, operational resilience must be dynamic and adaptive.

Operational resilience is as much about enabling positive outcomes as preventing negative ones. Confidence in the continuity of vital services underpins sustainable growth. By ensuring that financial services are reliable even in times of stress, operational resilience fosters trust, supports market functioning, and underpins confidence that businesses and consumers need to transact, invest, and thrive. Financial Market Infrastructures (FMIs) are central to this, facilitating the safe and efficient execution of clearing and settlement of transactions. The Bank of England ('the Bank') regulates FMIs to ensure these services remain robust and resilient.

The Bank has a dedicated regulatory regime for the operational resilience of FMIs, placing direct responsibility on boards and senior management to ensure that FMI operations can withstand and recover from disruption. March 2025 marked a significant milestone, with the full implementation of the Bank's Operational Resilience Policy. FMIs should now have identified their most important business services, defined impact tolerances for disruption of such services, and demonstrated, through rigorous testing, that they can recover within those tolerances under extreme but plausible scenarios.

Our supervisory approach continues to evolve. We are engaging with FMIs on how they meet these expectations, with feedback becoming more focused and specific, as part of our outcomes-based and technology-agnostic approach. This includes further steers on the types of recovery capabilities we expect from FMIs for 'extreme but plausible' scenarios, and the identification and prioritisation of critical elements of their services whose continuity is most essential to the financial system. This ensures our supervisory approach remain clear and proportionate, and focuses on what matters most for financial stability.

Alongside the Operational Resilience policy, the Bank of England, with other UK authorities, has introduced targeted policies aimed at addressing third-party and wider ecosystem risks. This includes our Outsourcing and Third-Party Risk Management policy and the newly finalised regime for Critical Third Parties (CTPs) to the financial system. The Bank also recently published Fundamental Rules for FMIs, which specifically require firms to maintain sufficient operational resilience and places direct responsibility on them to ensure that disruption of their operations does not compromise the resilience of the wider financial system.

Operational resilience fosters trust, supports market functioning, and underpins confidence.

However, the UK Operational Resilience policy landscape is not static, and further developments are underway. The Bank, and other UK Authorities, intend to finalise Operational Incident, Outsourcing and Third-Party Reporting (lOREP) requirements later this year. These aim to standardise incident notification and third-party register requirements, enabling better trend analysis and more effective identification of systemic risks. In parallel, given the evolving threat landscape, the Bank is also due to publish a consultation on further Information and Communication Technology (ICT) and cyber resilience guidance for FMIs.

International collaboration remains central to our agenda. Regulators are working together to harmonise standards, exchange best practices, and coordinate responses to cross-border risks. The Bank's forthcoming lOREP framework is designed to be as interoperable as reasonably practicable with both the EU's Digital Operational Resilience Act (DORA) and the FSB's Format for Incident Reporting Exchange (FIRE), and we are also mindful of international consistency in our upcoming cyber guidance. This alignment promotes consistency in regulatory expectations and enhances cross-border supervisory cooperation. To further champion international engagement and coordination, the Bank plays an active role in key international forums and standard setting bodies, including the Committee on Payments and Market Infrastructures (CPMI) lOSCO Operational Resilience Group. At the domestic level, the Bank and UK authorities continue to promote industry-wide testing, such as Sector Simulation Exercises (SIMEX), Cyber Stress Tests, and CBEST intelligence-led security testing, to assess FMIs' operational readiness for disruption, and maintain vigilance against emerging system-wide risks.

Operational resilience is a constantly evolving discipline requiring leadership, investment, and a willingness to challenge assumptions. By embedding resilience at the core of financial infrastructure, regulators and market participants can ensure that the system remains robust, responsive, and ready for the challenges and opportunities ahead.

NATHALIE PAULINE TUXEN
Head of Infrastructure and Cyber – Danmarks Nationalbank

Strengthening cyber and operational resilience in the financial sector

The financial sector plays a crucial role in society, and advanced cyberattacks on a financial institution can potentially threaten financial stability. Geopolitical tensions influence the cyber threat landscape increasing our focus on cyber-attacks as well as hybrid attacks. It is a complex task to enhance resilience. It requires ongoing efforts on multiple fronts: within individual companies, collectively in the financial sector and across sectors given the financial sector's dependence on electricity, telecommunications and key service provides.

Over the years, companies in the financial sector have been working diligently to enhance their cyber resilience, both individually and collectively in the sector.

At Danmarks Nationalbank, we have prioritized addressing cyber risks and other operational risks in collaboration with the Danish financial sector since 2016. The joint efforts of the financial sector are conducted within the framework of our public-private collaboration forum, named Financial Sector Forum for Operational Resilience (FSOR). Members of FSOR include systemically important banks, data centers, critical payments infrastructure owners, representatives from the insurance and pension sectors, key authorities and the forum is chaired and led by Danmarks Nationalbank.

In FSOR, Danmarks Nationalbank and the Danish financial sector take a risk-based approach to operational risks that may threaten financial stability. We conduct a bi-annual risk analysis at sector level which firstly ensures a common view on threats and vulnerabilities and secondly helps us prioritize our scarce resources towards the most important mitigating actions.

An important contribution to strengthening resilience in a financial institution is to test the effectiveness of the institutions security controls. In 2018 Danmarks Nationalbank implemented a TIBER-DK[1] program in agreement with the financial institutions who voluntarily committed to test according to the program.

TIBER tests are conducted in actual live production systems, i.e., ethical hackers test the defense in the critical systems that support the daily activities in the financial sector in banks, payments systems etc. During a TIBER test, the financial institution will identify, prevent, and respond to the ethical hackers advanced cyberattacks and afterwards withdraw learnings from the test in order to protect societally critical activities and reduce damages from attacks.

Strengthening resilience requires a continuously effort both on prevention and contingency planning.

In Denmark, we have been conducting tests on a continuous basis since 2018 generating important learnings. Now in 2025, the tests will continue mandatory. The Digital Operational Resilience Act (DORA) mandates threat-led testing (TLPT) for significant financial entities in the EU, with Danmarks Nationalbank being the authority for TLPT in Denmark.

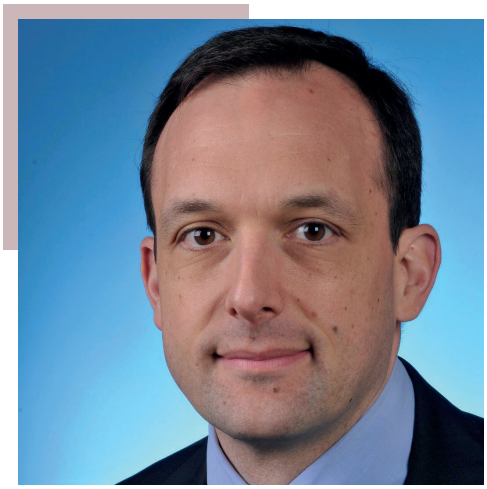
Danmarks Nationalbank is also working on a stress test of operational resilience at the sector level in collaboration with the Danish Financial Supervisory Authority. This test supplements the TIBER-tests. The purpose is to examine how individual institutions handle a large-scale, long-term operational IT incident in collaboration with other institutions in the financial sector, FSOR's crisis management, and relevant authorities.

A central focus area for strengthening cyber resilience is the financial sector's work on contingency plans, which aim to enhance individual companies' ability to continue the most critical operations even in extreme, plausible scenarios, like a comprehensive destructive cyberattack.

Contingency planning is another focus area in Danmarks Nationalbank's work. This includes monitoring central payment systems and payments solutions and working on joint initiatives to ensure business continuity and recovery for the most critical societal activities in extreme but plausible scenarios. One example is the establishment of a nationwide contingency plan for offline card payments in Denmark, which will ensure basic consumer capabilities for at least a week.

A lot of good work has already been done to strengthen operational resilience in the financial sector. And we have more work ahead. The threat landscape is evolving. Companies and authorities must adapt in order to limit damage of hostile attacks. This includes both work which can prevent incidents from materializing but also work which limits and handles the impact of serious incidents should they materialize.

1. *TIBER is short for Threat Intelligence Based Ethical Red team testing. TIBER-DK is in accordance with the TIBER-EU framework built by the ECB.*



THIÉBAUT MEYER
Director, Office of the CISO – Google Cloud

Strengthening financial sector resilience in a dynamic cyber landscape

Cooperation is key to effective CTPP oversight

Google Cloud welcomes DORA and is actively engaged in readiness preparations, viewing direct regulatory oversight as an opportunity to enhance understanding, transparency, and trust, ultimately strengthening operational resilience within Europe's financial sector.

Effective implementation requires taking account of the distinct operating models for ICT providers, especially cloud service providers (CSPs). Unlike traditional financial entities, CSPs have distinct structures, rapid development cycles, and specialized models, such as the shared responsibility one. Large CSPs like Google Cloud operate at an unparalleled scale, offering secure, resilient, and continuously updated infrastructure. The global footprint, with investment in cutting-edge security technologies, exceeds what individual financial entities can achieve independently.

Google Cloud advocates for flexible, proportionate regulations that accommodate rapid technological change and focus on outcomes, not prescriptive methods, which can stifle innovation crucial for Europe's growth. Avoiding overlaps and conflicts within the dual oversight structure (National Competent Authorities for financial entities, European Supervisory Authorities for CTPPs) demands dialogue and a pragmatic, risk and principle based approach from regulators. Additionally, harmonization should go beyond boundaries. For example, while frameworks like EU DORA and UK CTP have similar objectives, their differing requirements and scopes present challenges to international consistency.

Navigating the evolving cyber threat landscape

The cyber threat landscape is more perilous than ever before. We are witnessing an escalation in cyber pressure from highly skilled attacker groups globally, with the financial sector as a primary target. According to the Mandiant M-Trends 2025, the financial sector was the most targeted industry in 2024 with 17.4% of all cyber attacks, compared to other industries. According to the ENISA Threat Landscape: Finance Sector 2024 report, a significant number of publicly reported incidents occurred in the EU and neighboring countries during the last year, with most of them affecting at least one EU Member State.

Given this borderless nature of cyber threats, robust and continuous international cooperation is a necessity. Information sharing, particularly through established forums like FS-ISAC, is critical for the rapid dissemination of threat intelligence and best practices. Google Cloud actively contributes by publishing threat intelligence reports and offering incident response services through Mandiant, part of Google Cloud. Establishing common standards for data sharing would enable a more effective response to cyber threats and operational disruptions.

Embracing cloud for evolving cyber threats

CSPs like Google Cloud are at the forefront of this evolving landscape, deeply committed to strengthening the operational resilience of the financial ecosystem. Google Cloud strives for best-in-class security and actively invests in advanced security technologies, including AI and machine learning, to enhance threat detection and response capabilities for customers. AI can enable the automation of repetitive tasks, allowing our customers to focus on more complex activities, and can be used to analyze large volumes of security data, identify patterns, and automate responses to security alerts thereby reducing the risk of cyber threats.

Google Cloud's holistic security offerings, including Mandiant, aim to bring customers' security lifecycle into a DORA-ready state, addressing the demand for automation and cost reduction amid cybersecurity risks and staff shortages. DORA is seen as a key response to increasing cyber risks, requiring a true resilience mindset beyond mere "tick the box" compliance. Considering particularly that cyber risk and insurance is a board-level concern, Google Cloud's Risk Protection Program with our partners offers specialized cyber insurance policies, directly contributing to financial sector resilience by enabling effective risk mitigation. Cyber insurance is a critical component of a comprehensive defense strategy and this program provides additional support for financial entities in this dynamic environment.

> Fostering global cybersecurity in the financial sector is like building an interconnected dam.

Fostering global cybersecurity in the financial sector is like building an interconnected dam. CSPs act as advanced engineering firms, offering stronger materials and construction techniques, while DORA provides the blueprint for a unified, resilient structure. International cooperation ensures consistent monitoring and shared knowledge of effective dam-building and flood-control, preventing a single breach from compromising the entire system. In this ecosystem, all parties must partner towards the common goal of operational resilience.

Fireblocks

DEA MARKOVA
Director of Policy – Fireblocks

JASON ALLEGRANTE
Chief Legal & Compliance Officer – Fireblocks

How is tokenization changing custody and cybersecurity paradigms?

The tokenization of payments and investment instruments, and the growing adoption of crypto-assets, are presenting financial institutions with a new threat paradigm. More so than digitalization, tokenization is compelling banks, asset managers, and crypto-asset services providers to ask themselves: how am I protecting my clients' assets?

Evolving threat landscape

Protecting any tokenized asset means protecting the private keys that control it. This is a fundamentally different security objective from the traditional custody of financial assets in the digital age.

In parallel, cyberattacks are increasing in sophistication and involvement of state actors. AI-turbocharged social engineering, the rise of quantum computing, cross-chain vulnerabilities, and deepfake-enabled fraud expand the attack surface.

This faces regulators with a challenge. How to achieve a new security objective consistently, in a new industry?

Examples from abroad

Some non-EU regulators, particularly across APAC, have chosen to prescribe how firms manage the so-called hot and cold storage of digital assets. That is, what part of clients' assets should be held in a transactional hot online crypto wallet, and what should be kept in a safer offline cold wallet.

Our experience is that that level of prescriptiveness creates a false sense of security. For example, it is perfectly possible to segregate assets in an offline wallet, and still make the access point to this wallet so risky or so concentrated in a single point of vulnerability that the offline segregation is not safer at all.

Custody best practices

This is why in our industry we use terms like "defence in depth" and "zero-trust architecture". We refer to layers and layers of safety checks, each, by design, assuming that the previous layer had been compromised. This is comparable, in principle, to having multiple lines of defense in a risk management model.

We believe there are five pillars to effectively protecting private key materials:

- Cybersecurity: addressing cybersecurity risk management, strategy, and governance, as it relates to digital assets;
- Access management: defining and limiting user access privileges on a risk basis;
- Incident management: having detection, response, and investigation management for digital assets operations and transaction processes;
- Continuity: having policies, processes, and procedures related to business continuity, disaster recovery, and resolvability to ensure the availability and functionality of services in the event of a disruption to business activities.
- Key Management: making sure their key management and wallet management operations meet industry standards.

Industry experts will recognise that most of these elements are already addressed in DORA. However, our first observations on the market are that the industry, and possibly supervisory teams, do need further guidance on how to effectively translate these policy principles in operational realities specific to the nature of safekeeping digital assets.

To give one example, while DORA requires testing ICT risk scenarios, standardized testing protocols (e.g., red teaming) and alignment to continuity metrics such as recovery time objectives should be included in this guidance.

Evolution of the custody landscape

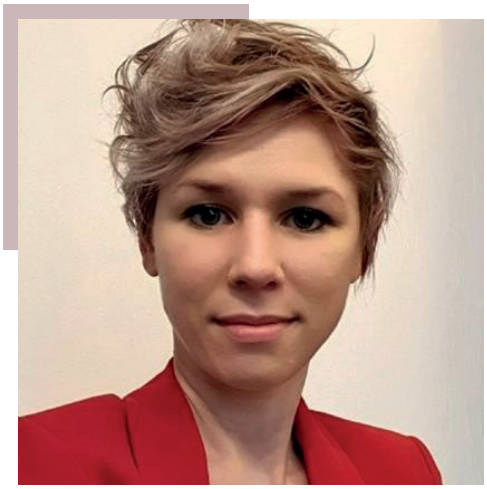
Another dimension to this topic is the evolution of the digital asset custodian's role and the role of its third-party technology partners.

The EU is familiar by now with the concept of hosted and self-hosted wallets. However, MiCA also introduces the choice of direct custody or reliance on third-party regulated custodians. This is a commercial, regulatory, and security choice. As of end-July 2025, 70% of authorised CASPs under MiCA have chosen to obtain a regulatory permission to deliver custody services directly to their EU customers.

> For safe tokenization at scale, advancements in technology and direct custodial models are critical.

These direct custodial setups still involve a trusted third party. In these cases, however, the role of the trusted third-party is limited to that of a technology service provider, while the CASP retains control and possession of the digital assets as well as the relationships with the end consumer.

Around the world, many market participants have come to believe in the superiority of these "direct-custodial" models because, among other reasons, they are native to the task of digital asset management, result in a near total elimination of counterparty risk to a custodial entity, and enable a higher degree of control by the asset owner. For example, institutions could set security standards programmatically based on not just key management and operations configurations, but also through transaction authorization policies that automate workflows in a manner not possible with traditional custodial transaction execution. This departure marks a major technological innovation.



VALÉRIE HÖSS
Head of European Affairs
– Commerzbank AG

Digital operational resilience and cyber risk – on ongoing journey

In 2020, the European Commission proposed DORA, with the aim to address the regulatory fragmentation and create an end-to-end framework for digital operational resilience and cybersecurity in the financial sector. Now, almost 5 years later, it is live.

Everyone in the same boat

As a first, DORA covers the whole ICT value chain, including ICT assets, systems and third party service providers, clearly integrating cybersecurity into the ICT risk management realm. Timing seems on point as in 2024 roughly 67% of operational payments incident reports filed under the PSD2 in Germany are linked to incidents at suppliers rather than the financial institution. And while the holistic view is a much-needed shift in how we approach ICT risk, this has also proven to be one of the challenges for implementation. With roughly 15.000 ICT service providers in the EU, the number of agreements to be reviewed and renewed was significant. And the volume is just one aspect: Acting in a highly regulated sector, financial institutions are well familiar with the interpretation of detailed regulatory requirements, the design and implementation of rigid internal governance and control frameworks, and supervision. However, this is not the case for all parts of the ecosystem. Onboarding processes and contractual negotiations not only take time, but they also require resources on both sides. Specifically for smaller providers, the increased scrutiny can pose challenges, in particular when they are confronted with a variety of questionnaires and contractual amendments at the same time. And implementation does not stop there: Testing requirements for the testing of ICT business continuity plans include the testing of services provided by third-party service providers as well.

The relevance of third party providers for the security and resilience of the financial sector is not only addressed through rigid third party risk management requirements. The direct oversight regime for Critical Third Party Service Providers (CTPPs) can play an important role as well. To create synergies and reduce operational burden without compromising security, close cooperation between supervisory authorities and supervised entities is key. Continuous flow of information not only from financial institutions to authorities, but also the other way around and the possibility to rely on examination findings could provide operational relief for all sides.

But ultimately, the key is to understand that operational and cyber risk of the financial sector does not exist in a vacuum and to act accordingly. Taking a holistic approach to the ecosystem and holding all parts of the value chain accountable is an important step. The regulatory framework also needs to focus on actual risk rather than compliance so that institutions can concentrate on managing incidents is another. This also means that rules for different parts of the economy are compatible and complementary, not duplicative – from regulation to supervisory practice. Reporting requirements are part of DORA, the AI Act, the GDPR and the Cyber Resilience Act. With different timelines, templates, thresholds. And even within the AI Act, one institution may be facing multiple supervisory authorities within a single jurisdiction, creating complexity and uncertainty.

Looking ahead – cyber and ICT risk evolve

The overall risk and cyber threat environment continues to evolve, but we witness an evolution, rather than a revolution. Due to growing geopolitical tensions, there is an increasing number of attacks against the infrastructure of banks, and since the beginning of the war in Ukraine, this development has been reinforced. Different forms of social engineering are still among the most common drivers for cyber-attacks. But as technology continues to evolve, cyber-attacks become increasingly sophisticated. The use of AI accelerates the identification and exploitation of weaknesses. Ransomware attacks are on the rise and those trends are expected to continue. What's new: growing availability of sophisticated technology industrialises cybercrime – creating significant efficiency gains for attackers, improving the quality of impersonation via video and voice deepfakes, and removing the need for technological and cyber expertise on their side. "Cybercrime-as-a-service" one could say. Combined with disinformation and social media, risks for financial stability may be exacerbated. The impact of those hybrid threats should be on our watchlist.

Operational resilience and cybersecurity are a team effort - every part of the ecosystem has a role.

Clearly, as cyber risks continue to evolve, so should the tools we use to fight them. It is however important to understand that AI is not a panacea: Large Language Models can create efficiency gains through automation. For cybersecurity purposes, machine learning can be used to identify anomalies or patterns, wherever large amounts of data are being processed. And we should not forget the human factor: where technology is unable to identify an attack, it's often us, who can be the deciding barrier.