Front of Mind: Operational Priorities in H2 2025

Vixio Regulatory Intelligence Outlook

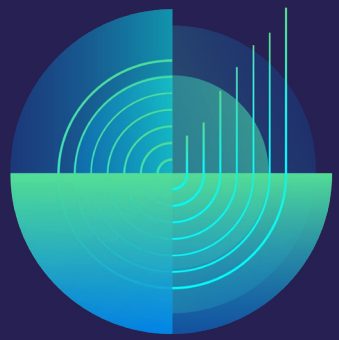
VIXIO

Analyse. Anticipate. Accelerate.

About This Report

This report is part of Vixio Regulatory Intelligence's Outlook series, which provides subscribers with forward-looking insights and consolidated research on key segments of the global financial services industry.

This edition is designed to provide high-level intelligence on operational resilience in 2025.



Contents

Authors

Writing/Editing:

Adam Parkinson | Editor

Jimmie Franklin | Senior Journalist

Louise Coleman | Chief of Staff

Design:

Alexandra Gibbs | Content Operations Analyst

Executive Summary

As we reach the midpoint of 2025, the year's key themes in regulatory and operational compliance in European financial services have crystallised.

Vixio has identified four key operational challenges that banks and other financial institutions operating in the EU and the UK will need to prioritise during the second half of the year:

- Operational resilience
- Cybersecurity
- ISO 20022
- Uncertainty

As they look to make the most of the remaining months of the year, organisations need to ensure they are in compliance with a range of regulation and legislation intended to bolster the financial services sector against a range of threats, as well as to increase efficiency.

Operational resilience

Operational resilience has come to the fore as digitisation has become a top priority for UK and EU financial services organisations that wish to remain competitive.

Regulations such as the EU's Digital Operational Resilience Act (DORA) and the UK's operational resilience regime are designed to strengthen financial institutions' ability to prevent, respond to, and recover from digital disruptions.

They are intended to ensure that banks, investment firms and a range of other financial entities can withstand, respond to, and recover from disruptions such as cyberattacks or system failures.

They aim to achieve this by strengthening operations between financial institutions and their ICT suppliers, and establishing harmonised regulatory frameworks that feature robust testing, including obligations for threat-led penetration testing, scenario-based stress testing and clear ICT risk governance frameworks.

Regulators are seeking to mitigate the industry's reliance on cloud services, technology partners and other third-party providers, which has increased exposure to operational risks outside firms' direct control.

They also emphasize the importance of ensuring that the risks identified in firms' severe but plausible scenarios are regularly updated to stay on top of the evolving threat.

For example, the UK's Financial Conduct Authority (FCA) recommends using horizon scanning to understand new and emerging risks, and make sure that "controls are in place to detect, respond and recover from operational disruptions, both current and in the future."

Events such as the CrowdStrike outage in 2024 and a series of outages at UK retail banks have only stiffened regulators' resolve when it comes to imposing higher standards of operational resilience. These incidents exposed gaps in contingency planning and communication protocols, areas now under greater regulatory scrutiny.

To meet heightened supervisory expectations, banks and other financial institutions must proactively assess their end-to-end operational processes, not only to minimise disruption, but also to avoid reputational and regulatory fallout.

Source: Ivan Marc | Shutterstock

Cybersecurity

Another key challenge for banks and other financial institutions in H2 2025 is closely linked to operational resilience: countering the risk of cyber-attacks.

Rising reliance on digital infrastructure, increasing interconnectivity with third parties, and heightened geopolitical tensions have all contributed to an increase in cyber threats facing financial institutions.

The types of threats are growing and morphing, with bad actors continuously developing new methodologies, including ransomware, deepfake-enabled social engineering, and exploitation of known vulnerabilities in widely used software.

In addition, those bad actors vary in type and motivation — they are not only criminals seeking to enrich themselves, but also nation states looking to cause problems in Europe and so-called 'hacktivists' who want to create disruption in the financial services sector to make a point. These diverse actor profiles present different challenges from a detection, attribution and mitigation standpoint.

With organisations facing not only financial losses, but also reputational damage and potentially enforcement action, defending against cyber-attacks has to be a priority.

And it is not only financial organisations that need to be vigilant: the threat takes in all types of business and even national security and public safety.

We have already seen attacks on infrastructure, which could fundamentally damage public trust, and regulators and governments in Europe and around the world are formulating their responses.

For banks, it will be important in the second half of 2025 to ensure that they have considered the impact of the EU's Network and Information Security Directive 2 (NIS2), an update to the legislative cybersecurity framework across member states.

Although financial services providers such as banks are not themselves in scope, being covered by DORA, the directive has important indirect implications for this type of institution. Their dependence on third-party ICT service providers, many of which fall directly under NIS2, means financial institutions will likely face indirect regulatory pressure to assure compliance through their own vendor risk management programmes.

Organisations should enhance their third-party risk frameworks to incorporate NIS2-related obligations, particularly around incident response coordination, secure data exchange and vendor contract terms.

They should also conduct end-to-end reviews of their cybersecurity frameworks to ensure they are defensible, tested, and proportionate to the institution's risk profile as cyber threats continue to grow.

ISO 20022

Another critical operational milestone for the second half of 2025 is the transition to ISO 20022, which has wide-ranging implications for payments infrastructure integrity, compliance and competitive positioning.

A key deadline for the global financial messaging standard is coming up in November, when the transition phase during which financial institutions could gradually adopt the new standard without disrupting their existing operations comes to an end.

This period began in March 2023, when Swift introduced support for ISO 20022 messages. Since then, organisations have been able to use both the new standard and traditional MT messages, but from the November 2025 deadline, all interbank payment messages must use ISO 20022 exclusively.

Organisations that have not transitioned risk being unable to process interbank payments, with knock-on impacts on liquidity management, customer experience and regulatory scrutiny.

Although the standard is not strictly regulation, banks and financial institutions should approach its application with the same degree of rigour.

The goal is to improve the efficiency, security and interoperability of global payment systems, which corresponds with the general aims of financial regulators.

ISO 20022 should ensure that the data in payment messages is more detailed, and better structured, improving automation, fraud detection and compliance processes. The enhanced data richness should support improved KYC/AML monitoring, more granular sanctions screening and audit traceability, which align directly with regulatory expectations for financial crime controls.

Its implementation represents a significant challenge for financial organisations, given the degree of technical complexity involved, the potential need to overhaul legacy systems and the likely impact on multiple areas of the business.

Firms lagging behind could face heightened scrutiny from both regulators and counterparties, particularly where ISO 20022 implementation intersects with transaction monitoring and cross-border payments compliance.

In addition, it is important that even those organisations that believe they are on track have clear oversight of the transition, because any shortcomings are likely to be exposed.

Any banks that fail to implement the standard by the deadline will be at a significant competitive disadvantage, and will also be exposed to operational failures that undermine their broader resilience strategies, particularly as digital payments become increasingly real-time and data driven.

Uncertainty

The final key challenge facing banks and other financial services organisations in the second half of 2025 is the biggest and most complex, building on the others and drawing in many other themes and threats.

The Trump administration in the US has been hugely active since the start of the year, and has upended a whole range of certainties at home and abroad.

Tariffs, deregulation and the promotion of cryptocurrencies all create questions for European financial organisations, which will have to closely monitor events to see how EU and UK regulators adapt to the new situation.

Banks face risks from a wide range of sources as the established international order fragments, creating opportunities for bad actors that will seek to take advantage of any weaknesses in firms' operations, including their cybersecurity.

In addition to these challenges, the rapid move of artificial intelligence (AI) tools into mainstream use creates both opportunities and threats for European banks.

Many organisations are already using such tools, which have the potential to dramatically improve the efficiency and effectiveness of systems, including enabling faster and more accurate threat detection.

AI's ability to analyse large volumes of data in real time and flag unusual patterns could be a gamechanger for fraud detection and prevention.

However, the flipside is that criminals also have access to AI and are increasingly taking advantage of the opportunities it offers to create more sophisticated scams.

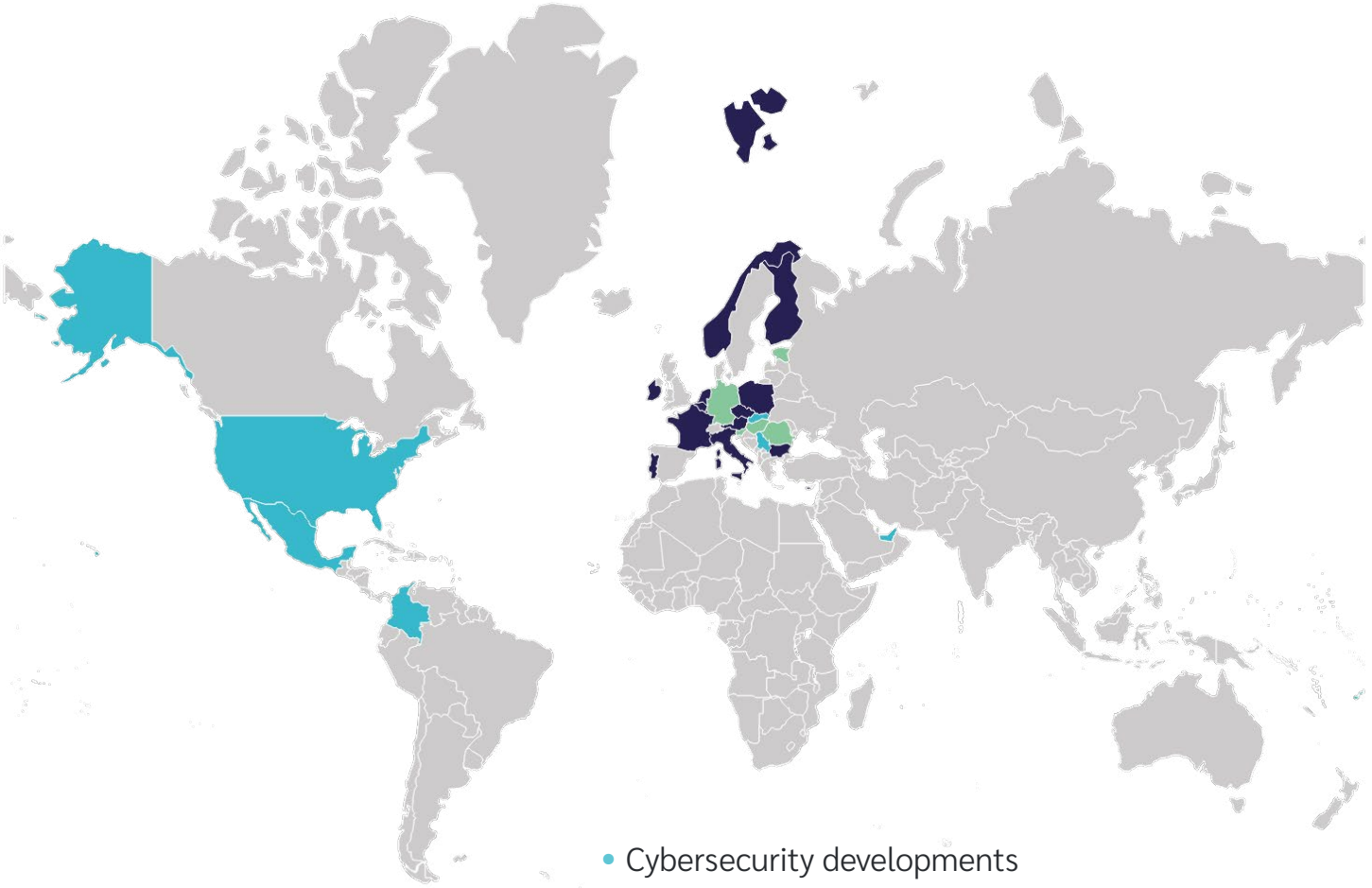
Source: VideoFlow | Shutterstock

The EU is leading the way on regulation in this area, with the AI Act the first comprehensive regulation on AI by a major regulator anywhere in the world. However, other countries, such as the United Arab Emirates and the UK, are gaining ground, with financial regulators regarding AI rules as an area that can spur innovation.

Nevertheless, the pace of change will throw up new challenges and risks, so banks should be vigilant through the second half of 2025.

Financial organisations need to prepare for the impact of uncertain geopolitics, regulatory change, the increasing threat of cyber-attack and the extensive use of emerging technology such as AI and quantum computing that have the potential to change the way markets operate and are regulated.

Cybersecurity and DORA Developments (2025 so far)



- Cybersecurity developments
- DORA developments
- Cybersecurity and DORA developments

Vixio's Horizon Scanning: Notable Numbers

77 Cybersecurity updates have been published in 2025

55 Digital Operational Resilience Act (DORA) updates have been published in 2025

Data collected as of May 6, 2025

Operational Resilience

Digitisation is now all but unavoidable for UK and EU financial services organisations that wish to remain robust and competitive.

The sector's rapid digitalisation and reliance on cloud services, technology partners and other third-party providers has increased exposure to operational risks outside firms' direct control.

As a consequence, operational resilience has risen up the agenda for regulators, and must therefore be a priority for financial organisations.

The expectations on the financial sector have increased significantly with the introduction of frameworks such as the EU's Digital Operational Resilience Act (DORA).

The goal of such regulations is to ensure that banks, investment firms and other financial entities can withstand, respond to, and recover from disruptions such as cyber-attacks or system failures.

Regulators have grown increasingly concerned about the dependencies that have become apparent with incidents such as the CrowdStrike outage in 2024, which have exposed gaps in contingency planning and communication protocols.

In addition, issues such as concentration risk have come to the fore, given that many critical services are being provided by just a handful of large tech firms.

Throughout the second half of 2025, banks and other financial services organisations will need to focus their attention on compliance with operational resilience requirements to avoid outages and other significant ICT incidents.

With supervisory expectations increasing, banks and other financial firms must proactively assess their end-to-end operational processes, not only to minimise disruption, but also to avoid reputational and regulatory fallout.

Any organisation that fails to comply with the DORA risks serious consequences, including fines, temporary shutdown and reputational damage.

The fines in particular have the potential to be highly damaging — they can be as much as 2% of the sanctioned firm's global annual turnover or €10 million, whichever is higher.

What is DORA?

The Digital Operational Resilience Act (DORA) is an EU regulation that provides a cyber and operational resilience framework for the EU's financial sector.

It has a wide-ranging scope, applicable to almost all of the financial services sector, from crypto-asset service providers to wealth managers.

Originally proposed by the European Commission as part of the Digital Finance Package in September 2020, it came into force in January 2023, with full compliance required by January 2025.

At the time of writing, 21 of the 27 member states had transposed DORA into national law. Belgium, Bulgaria, Spain, France, Latvia, and Portugal are all yet to do so.

National Transposition of DORA by EU Member States, May 2025

Member State	Transposition Deadline	Number of Measures
Belgium		0
Bulgaria		0
Czechia	**17/01/2025**	**19**
Denmark	**17/01/2025**	**8**
Germany	**17/01/2025**	**1**
Estonia	**17/01/2025**	**9**
Ireland	**17/01/2025**	**2**
Greece	**17/01/2025**	**1**
Spain		0
France		0
Croatia	**17/01/2025**	**37**
Italy	**17/01/2025**	**1**
Cyprus	**17/01/2025**	**11**
Latvia		0
Lithuania	**17/01/2025**	**2**
Luxembourg	**17/01/2025**	**1**
Hungary	**17/01/2025**	**17**
Malta	**17/01/2025**	**7**
Netherlands	**17/01/2025**	**2**
Austria	**17/01/2025**	**1**
Poland	**17/01/2025**	**2**
Portugal		0
Romania	**17/01/2025**	**5**
Slovenia	**17/01/2025**	**3**
Slovakia	**17/01/2025**	**12**
Finland	**17/01/2025**	**13**
Sweden	**17/01/2025**	**13**

DORA establishes a harmonised set of rules for ICT risk management, incident reporting and resilience testing.

Third-party risk oversight is also part of the package, particularly for cloud computing firms and other critical technology providers. This will increase scrutiny of financial services firms' contractual relationships with bigtech players such as Microsoft and Amazon Web Services.

Under ICT risk management requirements, financial institutions are required to implement resilient governance frameworks to identify, assess and mitigate cyber threats while also guaranteeing business continuity.

Meanwhile, incident reporting obligations mandate firms to detect, classify and report major ICT-related incidents to regulators within strict timeframes.

In addition, to assess resilience, DORA introduces threat-led penetration testing (TLPT), intended to ensure firms can withstand cyber-attacks and operational disruptions.

Financial services firms will need to simulate attacks on their systems so that they can better understand their weaknesses and correct the problem — before a criminal also identifies that weakness and takes advantage.

Key compliance challenges

Firms readying themselves to comply with DORA face a number of challenges.

One major obstacle is third-party oversight. Organisations must map all ICT dependencies and conduct thorough due diligence on suppliers, because if a third-party provider is not complying, then it could ultimately come back on them too. DORA will need to be factored into contracts on this topic.

Many financial entities rely on a small number of cloud providers, which creates significant risk concentration.

DORA requires firms to renegotiate contracts with these third parties to adhere to compliance requirements, and although many cloud providers with business in the EU will be aware of the regulation, this adds complexity to vendor management.

The resilience testing requirements, particularly TLPT, also demand substantial resources from firms, creating a financial and operational strain for smaller firms in particular.

For example, imagine a small investment firm, located in Cyprus. It has limited IT and compliance resources, and unlike larger financial institutions that have dedicated cybersecurity teams and budgets for regular testing, it lacks in-house expertise, meaning it needs to hire external specialists. This means less profit and less resource available for key operations such as client service.

Incident reporting deadlines are also tight, with major ICT incidents needing to be reported within hours, increasing the pressure on compliance teams.

Failure to report an incident within the specified time frame could result in public censures or fines from regulators, which might also require firms to bring in an external auditor for a temporary period.

This was the case with neobanks N26 and Solaris in Germany, which were found to have fallen foul of compliance requirements.

How resilient is the EU financial sector?

In the coming months and years the resilience of the EU's financial sector and how effectively the DORA framework can prevent issues arising will be put to the test.

Despite the spotlight on cyber defences, both financial services firms and EU authorities still have significant vulnerabilities to consider.

The financial sector is highly dependent on just a handful of bigtech cloud providers. If disaster strikes and an outage happens at one of these key providers, it could lead to disruption at multiple institutions.

In addition, small and medium-sized enterprises (SMEs) and fintechs may lack the resources to comply fully with DORA or to defend against sophisticated cyber-attacks.

Supply chain risks are also a concern, as even a resilient financial firm could be affected by an attack on a critical supplier.

If a cyber-attack spans multiple member states — and with both EU and national regulators increasingly concerned about geopolitical uncertainty — effective coordination will be key.

Any slow response will have a negative impact on reckoning with the damage.

Operational resilience rules in the UK

The UK's Financial Conduct Authority (FCA) and Bank of England have introduced operational resilience compliance requirements in a bid to ensure that financial institutions can withstand and recover from disruptions.

Firms supervised by these regulators are required to identify important business services, set impact tolerances and implement measures to remain within them.

By March 31, 2022, firms had to map dependencies and test their resilience frameworks.

By March 31, 2025, they had to demonstrate their ability to stay within impact tolerances under severe but plausible scenarios.

The regulators also expect firms to continuously review and improve their resilience strategies, ensuring they can operate effectively during disruptions.

Similarities with Europe, not a copy-and-paste job

The EU and UK frameworks have a similar emphasis on operational resilience, but firms should resist the temptation to simply copy their work on DORA in the UK, as the FCA's operational resilience rules differ in scope, structure and specific requirements.

Although both frameworks cover risk management, resilience testing and third-party oversight, the FCA's approach is more selective and focuses on firm-specific impact tolerances rather than DORA's broad, prescriptive regulatory package.

It is much shorter and less detailed than DORA, despite both striving for the same outcome.

Even where the rules overlap, their implementation differs, and direct replication is likely to leave the UK's regulators displeased, as it could signal laziness and a lack of interest in fully understanding the UK's unique regime.

Firms that operate in both jurisdictions should conduct a gap analysis to align their UK operations with FCA requirements, rather than assuming DORA compliance automatically satisfies UK rules.

Operational resilience is not a tick-box exercise, and firms operating in the UK must tailor their approach accordingly.

Cybersecurity

Like the rest of the world, Europe has had to face up to a widening array of cyber issues and threats.

Rising reliance on digital infrastructure, increasing interconnectivity with third parties, and heightened geopolitical tensions have all contributed to an increase in cyber threats facing financial institutions.

Digitisation can create efficiencies, but it also brings vulnerabilities, and governments and regulators across the region have had to act quickly to ensure that these vulnerabilities are dealt with.

The risks posed by cyber-attacks have grown increasingly severe, not only in terms of financial losses, but also in relation to national security, public safety and trust in digital infrastructure.

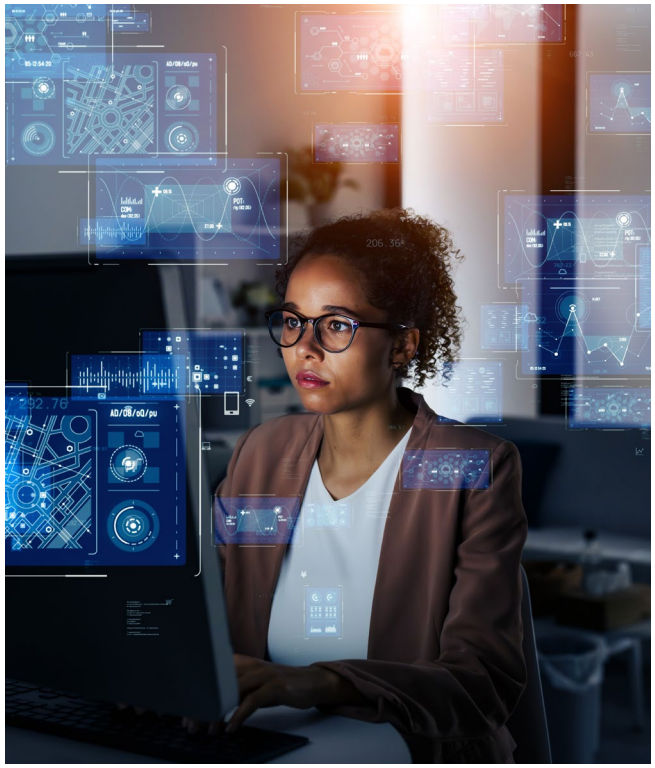
In addition, the types of threats are evolving, with bad actors continuously developing new methodologies, including ransomware, deepfake enabled social engineering, and exploitation of known vulnerabilities in widely used software.

Cyber-attacks in places such as transport systems and hospitals have shown that this is a meaningful threat, and even a potential form of warfare, that regulation must correspond to.

For banks and other financial institutions, ensuring that they — and their key suppliers — are in compliance with the relevant regulation must be a top priority for the remainder of 2025 and beyond.

They should conduct end-to-end reviews of their cybersecurity frameworks to ensure they are defensible, tested, and proportionate to the institution's risk profile as cyber threats continue to grow.

Falling short in this area leaves them vulnerable to both attack and enforcement action.



Source: metamorworks | Shutterstock

EU cybersecurity: DORA and NIS2

Much of the EU's cybersecurity regulation is covered by the Digital Operational Resilience Act (DORA), but the bloc has also tackled cyber resiliency via other legal frameworks.

A key recent example is the Network and Information Security Directive 2 (NIS2), the EU's updated legislative framework designed to shore up cybersecurity across member states. Passed by the EU's co-legislators in January 2023, member states were required to have completed transposition by October 2024.

NIS2 introduces stricter, more prescriptive compliance requirements than its predecessor, although only around half of the EU's member states have transposed it thus far.

National Transposition of NIS2 by EU Member States, May 2025

Member State	Transposition Deadline	Number of Measures
Belgium	**17/10/2024**	**2**
Bulgaria		0
Czechia	**17/10/2024**	**72**
Denmark	**17/10/2024**	**2**
Germany	**17/10/2024**	**12**
Estonia		0
Ireland		0
Greece	**17/10/2024**	**3**
Spain		0
France		0
Croatia	**17/10/2024**	**2**
Italy	**17/10/2024**	**1**
Cyprus		0
Latvia	**17/10/2024**	**1**
Lithuania	**17/10/2024**	**22**
Luxembourg		0
Hungary	**17/10/2024**	**24**
Malta	**17/10/2024**	**1**
Netherlands		0
Austria	**17/10/2024**	**2**
Poland	**17/10/2024**	**2**
Portugal		0
Romania	**17/10/2024**	**16**
Slovenia		0
Slovakia	**17/10/2024**	**9**
Finland		0
Sweden		0

The cyber regime replaces the original 2016 NIS Directive and in doing so significantly expands its scope to include more sectors, such as public administration, space, postal services and manufacturing of critical products.

These requirements include mandatory risk management practices, encryption, multi-factor authentication and regular security assessments.

A key feature is the obligation to report significant cybersecurity incidents within 24 hours of detection, followed by impact assessments and detailed updates.

Governance is also a priority, with senior management now required to take clear responsibility for cybersecurity strategy, compliance and investment.

Cybersecurity risk is integral to NIS2. The overhauled legal framework mandates measures such as vulnerability management, access control, supply chain security and zero trust architecture in a bid to raise baseline standards across the trading bloc.

These efforts aim to strengthen critical infrastructure and digital services against increasingly sophisticated cyber threats, which have targeted EU member states in recent years.

For example, in January 2023, Germany's Social Democratic Party (SPD) was targeted by the Russian hacker group APT28, which is affiliated with the Russian secret service. In this instance, the cyber attackers exploited a vulnerability in Microsoft software and were able to access sensitive data, prompting Germany to consider EU sanctions and diplomatic measures.

Another incident — one that could have been particularly impactful but for a mistake by the attackers — took place in March 2024 in France. The Russian-affiliated hacking group Sandworm mistakenly targeted a small mill in the country's Burgundy region, having intended to attack a hydroelectric dam, manipulating software to release water and lower downstream levels by 20 centimetres.

Impact on financial services

Although NIS2 does not directly regulate financial services providers such as banks, which instead are in scope of DORA, it still has important indirect implications.

DORA is tailored specifically to the financial sector, with compliance requirements surrounding ICT third-party risk and resilience testing, including threat-led penetration testing for critical firms.

Given financial institutions' dependence on third-party ICT service providers, many of which fall directly under NIS2, they will likely face indirect regulatory pressure to assure compliance through their own vendor risk management programmes.

They should enhance their third-party risk frameworks to incorporate NIS2-related obligations, particularly around incident response coordination, secure data exchange and vendor contract terms. If a supplier is not up to standard, it could reflect badly on the institution, and show an apparent lack of willingness to invest properly into cybersecurity protocols.

NIS2 and DORA share common goals, with similarities such as a focus on enhancing risk management, enforcing timely incident reporting and instilling senior leadership accountability.

Incident reporting timelines are similarly strict, and both frameworks promote cross-sector coordination on cybersecurity.

UK cybersecurity rules

The UK's oversight of cybersecurity has also been subject to reform.

On April 8, 2025, the UK Department for Science, Innovation & Technology (DSIT) released the Cyber Governance Code of Practice, which is intended to help boards and directors govern cybersecurity risks effectively.

Designed primarily for medium and large organisations in both the public and private sectors — and with broad application which could include financial institutions — the code provides a structured framework for integrating cyber risk into wider corporate governance.

It complements existing resources such as the Cyber Governance Training and Cyber Security Toolkit for Boards, forming part of the government's free support package.

The code highlights five focus areas for boards: risk management; strategy; people; incident response and recovery; and assurance and oversight.

Within each area, it outlines specific corporate governance actions. This includes defining a cyber risk appetite, embedding cyber strategies into broader business plans, fostering a strong cybersecurity culture, guaranteeing robust incident response planning and maintaining effective oversight structures.

The UK government has introduced the code because of the growing threat landscape, due to the rise in cyber attacks and also geopolitical uncertainty.

For example, the UK's cyber security breaches survey, published on April 9, 2024, found that 74 percent of large businesses and 70 percent of medium ones experienced cyber attacks in the preceding 12 months, and the code urges strong leadership involvement.

It also serves as the foundation for the DSIT's modular approach to cyber governance.

The government intends the code to be used in conjunction with other guidance, such as Cyber Essentials, the Software Security Code of Practice and the upcoming AI Cyber Security Code of Practice, so that there is a comprehensive, layered approach to building organisational cyber resilience.

Source: alice-photo / Shutterstock

Legislative activity

On taking office in 2024, the Labour government also announced the Cyber Security and Resilience Bill (CS&R). This is part of a global shift on cybersecurity, as in the US the Securities and Exchange Commission (SEC) announced the creation of the Cyber and Emerging Technologies Unit (CETU) in February 2025.

The CS&R will be the UK's flagship effort to modernise its cybersecurity legislation, and updates the existing Network and Information Systems (NIS) Regulations 2018.

Like the EU's NIS2 Directive, which the framework is derived from, the legislation widens the scope to include sectors such as transport, energy, healthcare, drinking water and digital infrastructure.

The bill also mandates stricter incident reporting, requiring significant cyber incidents to be reported within 24 hours, followed by a detailed report within 72 hours, closely mirroring the requirements of NIS2 to ensure regulatory alignment.

In addition to reporting obligations, the CS&R Bill underscores the importance of board-level accountability, and senior management will now be required to take active responsibility for cybersecurity strategy and oversight.

The legislation also places greater emphasis on managing supply chain risk, and obliges organisations to assess and mitigate vulnerabilities introduced by third-party vendors. This addresses consumer-level cybersecurity and imposes minimum security requirements on internet-connected devices.

For example, it bans weak default passwords and requires manufacturers to provide clear information on security updates.

The legislation also mandates mechanisms for reporting vulnerabilities, aiming to improve protection against threats posed by the proliferation of smart home technologies.

It is yet to pass. However, with Labour having such a hefty majority, and cybersecurity hardly being a polarising issue between the left and right of British politics, industry players should anticipate that this will be passed at some point during Labour's term in government. When that is depends on parliamentary time, but considering geopolitical issues and hacks such as that on hospitals, it is likely to be a priority.

"The first duty of this government is to keep its citizens safe. To anticipate the threats we face, minimise the risks we take, and make the UK as safe and secure as it can possibly be," said the UK's secretary of state for science, innovation and technology Peter Kyle in a policy statement on the matter. "That is what making National Security our number one priority means in practice."

In addition, the Product Security and Telecommunications Infrastructure (PSTI) Act came into force in April 2024.

Impact on financial services

As with the EU's cybersecurity rules, the code of practice and legislation such as the CS&R Bill increase banks and other financial institutions' obligations around supply chain risk, governance and incident coordination.

This is especially the case in relation to ICT dependencies, and for digital wallets, the PSTI Act raises the bar on device-level cybersecurity and consumer protection.

Although financial services organisations are not the immediate target of these regulatory changes, they will be affected via the stringent requirements for their third-party providers as it will mean reviewing contracts and for risk management reasons, ensuring full compliance from partners.

This may limit contracts with those not based in the UK, although UK and EU standards may become a prerequisite for companies overseas for commercial reasons.

Financial institutions will need to conduct the appropriate due diligence to ensure that they are in compliance and able to align their work with the new guidance and legal framework.

Vixio's Regulatory Radar Podcast

Vixio's Regulatory Intelligence's podcast brings together leading experts in regulation and compliance to provide the intelligence you need to anticipate and navigate global regulatory shifts.

The latest episodes of the podcast cover such topics as PSD3, responsible gambling demands, Brazil and authorised push payment (APP) fraud.

Visit vixio.com/podcasts for more information about the Vixio Regulatory Radar Podcast.

ISO 20022

The transition to ISO 20022 is a critical operational milestone for the second half of 2025, one with wide-ranging implications for payments infrastructure integrity, compliance and competitive positioning.

ISO 20022 is a global financial messaging standard crafted by the international payment messaging network Swift.

It has been designed to improve the efficiency, security and interoperability of payment systems globally, and provides a harmonised language and data structure for financial communications, replacing older formats such as Swift MT messages.

The standard allows for more detailed, more structured data in payment messages, improving automation, fraud detection and compliance processes. This enhanced data richness should support improved KYC/AML monitoring, more granular sanctions screening and audit traceability, which align directly with regulatory expectations for financial crime controls.

Swift introduced support for ISO 20022 messages on March 20, 2023, marking the start of a coexistence period where both ISO 20022 and traditional MT messages could be used.

This transition phase allows financial institutions to gradually adopt the new standard without disrupting existing operations.

This period will end in November 2025, at which point all interbank payment messages must use ISO 20022 exclusively, and legacy MT messages will no longer be supported.

ISO 20022 implementation should be an area of focus for financial services firms over the coming months, as falling behind in the implementation of the standard could put them at a significant disadvantage.

Organisations that have not transitioned risk being unable to process interbank payments, with knock-on impacts on liquidity management, customer experience and regulatory scrutiny.

Europe’s progress

The adoption of ISO 20022 is a significant development for financial institutions globally, with different regions and jurisdictions implementing the standard according to their specific timelines.

The standard is not a regulatory requirement, like the Instant Payments Regulation (IPR) or anti-money laundering (AML) rules in the EU and the UK.

However, it has been widely embraced and it makes sense for financial services organisations to think of it in a similar way to regulation, and apply the same degree of prioritisation.

Not implementing ISO 20022 properly could even be more financially damaging than failing to comply with key regulation, given the potential commercial consequences.

These include slowed down payments, higher fees from Swift and a competitive disadvantage to other organisations that have applied that standard correctly.

In the UK, the Bank of England successfully migrated CHAPS (Clearing House Automated Payment System), its real-time gross settlement payment system used for same-day electronic transfers between banks, to ISO 20022 on June 19, 2023.

Since this date, the central bank has outlined a phased approach for mandating enhanced data elements.

As of May 2025, the use of Purpose Codes and Legal Entity Identifiers (LEIs) will be mandatory for CHAPS payments between financial institutions, as well as Purpose Codes for property transactions.

Starting in November 2025, where remittance data is included in payment messages, it must be structured, and hybrid addresses will be permitted, with a move towards fully structured addresses by November 2026.

The European Central Bank (ECB) also migrated its TARGET2 system to ISO 20022 in March 2023.

Opportunities with ISO 20022

Despite the heavy lifting involved in replacing legacy systems, the new messaging standard offers plenty of opportunity for banks.

The structured data made available by ISO 20022 standards could enable regulatory compliance efforts, including AML and fraud prevention measures, by providing more detailed information within payment messages.

Data accuracy

Using traditional payment systems where addresses are often stored as unstructured text, a system may not differentiate between, say, “Havana Street, Florida” and “Havana, Cuba”.

In such a case as this, the bank’s sanctions screening system might mistakenly associate the transaction with “Havana”, the capital of Cuba, which is a jurisdiction subject to certain international sanctions.

This would trigger unnecessary payment delays and manual investigations, all for the sake of being compliant with sanction screening requirements.

ISO 20022 resolves this issue by structuring address data into distinct fields for street name, city, country and postal code, and with this increased level of detail, financial institutions are able to immediately distinguish between a legitimate transaction and one requiring further review.

Similarly, if a person or company shares a name with a sanctioned entity, richer data fields such as full legal names, dates of birth, tax identification numbers or LEIs allow banks to conduct more precise identity verification.

For instance, if a payment is made to “Alexander Petrov”, a name that appears on a sanctions list, structured data elements such as birth date and nationality will be able to confirm whether the individual is the sanctioned person or someone unrelated with the same name.

This reduces false positives and ensures that compliance teams focus only on genuinely suspicious transactions, making financial crime prevention less onerous.

Tackling fraud

ISO 20022 enables financial institutions to get ahead of criminals in the ongoing global fight against fraud, based on the fact that it allows the capture of richer data, including structured payer and payee details, invoice references and transaction purposes.

This makes it easier for banks to detect anomalies and potential fraudulent activity. For example, if a payment to a business suddenly lacks the usual structured invoice reference or includes unusual location details, the system can flag it for review.

Inconsistencies such as a company’s registered LEI not matching its listed address, will also trigger automatic alerts, helping banks prevent fraud before money is transferred.

Improved service

Adopting ISO 20022 will allow banks to offer improved services to corporate clients, such as better cash management and reconciliation capabilities.

The standardisation of messaging formats should make everything run more efficiently on a global scale by enhancing interoperability between banks, streamlining cross-border transactions and supporting the development of real-time payment systems across the world.

Time to act

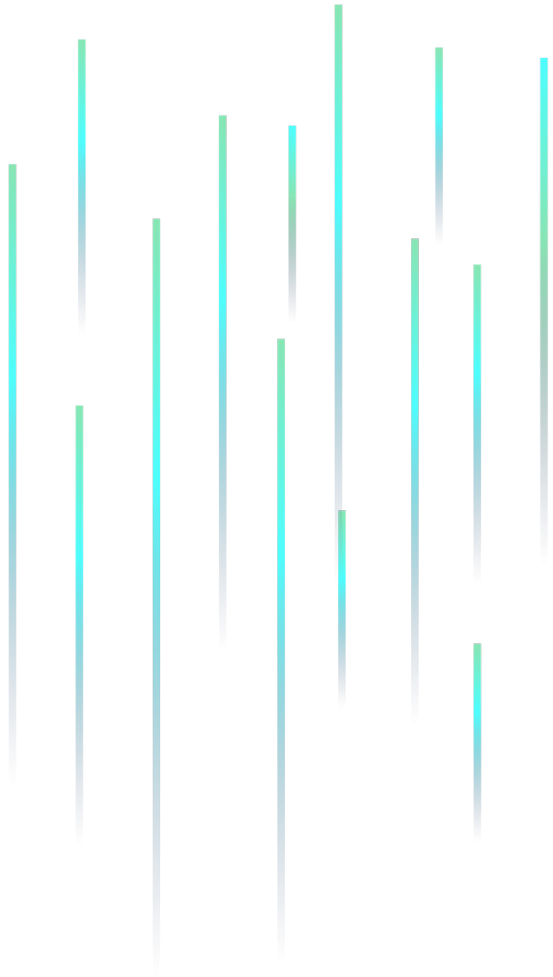
To be ready for the operational deadline in November, banks need to develop comprehensive plans to upgrade systems and processes to accommodate ISO 20022, if they have not already done so.

Institutions should assess their operational capabilities to handle the richer data formats and make sure that staff are trained to manage the new messaging standards.

Firms falling behind in the process could face heightened scrutiny from both regulators and counterparties, particularly where ISO 20022 implementation intersects with transaction monitoring and cross-border payments compliance.

If firms fail to ready themselves for the new messaging standard, there is a risk of key efficiencies not being achieved, and of a bottleneck developing as the deadline nears.

Organisations that do not implement the standard by the deadline will be at a significant competitive disadvantage, and will also be exposed to operational failures that undermine their broader resilience strategies, particularly as digital payments become increasingly real-time and data driven.



Uncertainty

We are in a period of rapid global change, with digitisation and geopolitical uncertainty having an impact on the legal frameworks and risks for financial services in Europe.

Now more than ever, banks need to consider not just their own resiliency, but also the potential risks from a range of sources, including the fragmentation of the international order and the threat from bad actors that seek to take advantage of weak or poorly designed cybersecurity structures.

The Trump administration's domestic and foreign policy decisions, including the imposition of tariffs and apparently warm relations with Russia are calling into question long-standing alliances and international norms.

Even if it never fully materialises, the prospect of a world where companies face higher costs for using US-based services could create significant challenges, particularly if firms find themselves priced out or unable to outsource to US third-party providers for work such as cloud management.

At the same time, firms are having to face up to the reality of a growing wave of cybersecurity threats, fuelled by increasingly sophisticated state-backed actors whose agendas often diverge sharply from European norms.

The potential for serious disruption, whether via a major bank outage or through a hacking scenario that sees funds disappear, has pushed cyber resilience to the top of boardroom agendas.

Even when a company is not at fault for a cyber-attack, the reputational fallout can be severe, and the financial consequences, including potential liability for damages, may be damaging.

Moving into the second half of 2025, financial organisations need to be taking into consideration a range of scenarios when planning and executing their operations.

The uncertain geopolitics and accompanying regulatory change mean that it would be easy to be caught off guard by new developments.

In addition, technology such as AI and quantum computing is reshaping the way markets operate and are regulated, creating both opportunities and threats for financial organisations.

All these developments will have long-term consequences, particularly for the unwary, so it is important that firms are alert to the issues in the immediate term to ensure they are compliant and secure for the future.

Preparing for disruption

In this digitised world, both regulators and financial services institutions face disruptive, even devastating, risks.

In a blog post, the UK Financial Conduct Authority's (FCA) tech chief, Suman Ziaullah, wrote that "the shutdown of Heathrow Airport from an electricity substation fire and last July's CrowdStrike outage exemplify the types of disruptions firms should prepare for, both in their impact on vital services and in the back-up plans needed when systems, processes and buildings are compromised".

This shows that the FCA wants the firms it supervises — across the board — to be alert to how badly things can go if they are not adequately prepared for different scenarios.

A bank unable to serve customers due to an outage, or an insurer dealing with an email hack exposing personal data, are both realistic scenarios that firms should grapple with.

And in a world that is becoming increasingly fractured, firms should be alert to how cyber resilience will be tested.

For example, there is every chance that the recent burst of geopolitical uncertainty could increase cybersecurity and operational resilience risks in several ways.

State-sponsored cyber-attacks are more likely during periods of tension, with countries such as Russia, China, Iran and North Korea using cyber operations for espionage, disruption and influence.

We are already seeing instances of this — in February 2025, hackers thought to be working for the North Korean regime successfully stole a record-breaking $1.5bn from the crypto company ByBit.

> *"The shutdown of Heathrow Airport from an electricity substation fire and last July's CrowdStrike outage exemplify the types of disruptions firms should prepare for, both in* ***their impact on vital services*** *and in* ***the back-up plans needed*** *when systems, processes and buildings are* ***compromised.***"
>
> **— Suman Ziaullah, UK Financial Conduct Authority's Head of technology, resilience and cyber**

The likely impact of AI

This is happening at the same time as an increased use of AI in financial services, which is a double-edged sword for the sector and its cyber and operational resilience.

AI can no doubt bring welcome efficiencies to firms in the push for greater resiliency, both from the private sector and regulators. For example, it enables faster and more accurate threat detection, as it can analyse large volumes of data in real time and flag unusual patterns.

Take a neobank in the EU that is digitally native and is comfortable investing in AI solutions. Its AI solution has picked up an unexpected surge in outbound network traffic from a subset of servers, and this is flagged as behaviour that does not match typical usage patterns. AI could quickly trigger an automated response that is able to isolate the affected systems while engineers investigate the root cause, and early detection is able prevent possible data leakage or service disruption, which could be spurred by a bug in the system or an attempted hack.

AI solutions are ultimately able to contribute to operational resilience through the continuous monitoring of critical systems for signs of performance issues or failures. They can simulate different risk scenarios, providing insights into how disruptions might unfold and how best to mitigate them.

The technology is also a useful tool in managing supply chain risk by assessing the resilience of third-party vendors and identifying potential vulnerabilities across extended networks.

However, deploying AI in these areas comes with significant risks.

Financial organisations' IT and compliance teams must remember that attackers can also use AI to their advantage. They can leverage it to automate attacks, create convincing phishing attempts, and bypass traditional security controls.

Poorly trained AI systems also run the risk of generating false positives or missing genuine threats, potentially undermining confidence in the technology.

Ultimately, despite AI's progress, the human touch is still absolutely vital for resiliency in financial services.

Source: NicoElNino | Shutterstock

The importance of harmonisation

In the coming years, we will likely see private sector players demanding greater coherence between different jurisdictions, with similar outcomes and expectations coming from regulatory regimes.

For example, in a more fragmented world, divergent incident reporting requirements across jurisdictions could end up creating a significant challenge to operational and cyber resilience.

Financial institutions operating internationally could face a complex web of inconsistent rules on what to report, how and when.

Such fragmentation could see inefficiencies continue, compliance costs increase and responses, which are critical for ensuring an attack is stopped, delayed. This undermines the very resilience frameworks regulators aim to strengthen.

Harmonisation is being promoted by some already, for example, via the EU's AI Act and DORA but also at a supranational level via international bodies such as the Financial Stability Board (FSB).

The FSB helps promote harmonisation by providing common standards and formats, such as the newly finalised Format for Incident Reporting Exchange (FIRE).

Standardised reporting frameworks improve the quality and consistency of the data shared with authorities, and can go some way to enhancing cross-border coordination and reducing the operational burden on firms.

In turn, this supports faster, more effective, incident response and a clearer view of systemic risks.

This is similar to ISO 20022, another type of global harmonisation that strengthens operational resilience and creates more efficiency.

As a widely adopted international messaging standard for financial data, this sort of convergence is necessary for making financial services both a safer and more optimised industry globally.

Banks and other financial services organisations should examine where such common standards can help them today, to be better prepared for what may be coming down the line.

Regulatory Intelligence

About Vixio Financial Services

Vixio is a leading Regulatory Technology (RegTech) provider that takes the heavy lifting out of regulatory monitoring. For nearly two decades, Vixio has offered comprehensive, actionable intelligence on compliance across over 180 jurisdictions worldwide. Our expert team combines deep industry knowledge with cutting-edge technology to provide critical insights to some of the world's biggest brands in the financial, payments and gambling industries. With Vixio's award-winning platforms, organisations can navigate the ever-evolving global regulatory landscape with ease to mitigate risk and uncover new growth opportunities.

UK Office
St Clare House, 30-33 Minories
London
EC3N 1DD
Tel: +44 (0) 207 921 9980

US Office
1250 Connecticut Ave NW Suite 700
Washington, DC 20036
Tel: +1 202 261 3567

info@vixio.com

Vixio.com

Disclaimer