CAPCO

REGULATORY HORIZON

2025 Edition 11



Contents

Geos Keys: UK | US/Canada | EU | APAC | Global

Foreword

Overviews

1. UK Regulatory Summary 5
2. US Regulatory Summary 10
3. Canada Regulatory Summary 15
4. EU Regulatory Summary 19
5. APAC Regulatory Summary 24
6. Regulatory Heatmap 29

Non-Financial Risk

7. The 2025 Omnibus package – EU push for simpler, smarter sustainability rules 31
8. ESG scenario analysis and long-term strategy 34
9. Adoption of the International Sustainability Standards Board (ISSB) standards: A closer look 37
10. Navigating the new EU Sustainability Regulations 39
11. Addressing customer vulnerability – the challenge continues 43
12. FS25/2: Transforming conduct risk management in the Consumer Duty era 46
13. Pure Protection Market Study 50

Operational Resilience & Cyber

14. Navigating the evolving landscape of AI regulation in regulated industries 53
15. Regulatory focus post implementation of the UK Operational Resilience policy and Digital Operational Resilience Act 58
16. Australia's Prudential Standard CPS 230 – Operational Risk Management 61
17. Cyber resilience in APAC: India & Hong Kong step up supervisory expectations 66
18. The Bank of Thailand raises the bar on high-risk transactions and sanctions exposure 70
19. Integrity and security: OSFI's No.1 risk for 2025 73
20. Financial Data Access regulation (FiDA) 78
21. India's Digital Personal Data Protection Act (DPDPA): Impact on the financial sector 81
22. The future of regulatory reporting for financial institutions: An oversight on the Integrated Reporting Framework (IReF) and the Banks' Integrated Reporting Dictionary (BIRD) 84

Click on the article name to go to the relevant pages. Click on the "back to contents" link on any page in the article to return to the start of the Contents list.

Contents

Geos Keys: UK | US/Canada | EU | APAC | Global

Financial Crime

23. Role of technology in financial crime prevention: FCA's perspective and industry innovations 88
24. Economic Crime & Corporate Transparency Act 90
25. Navigating the storm: Sanctions risks under the Trump administration 93
26. Navigating PSD3 – a financial crime perspective 96

Market Regulation

27. Transaction reporting: Harmonization and transformation through automation 99
28. Impact of deregulation in the US 103
29. US extended trading hours: Impact assessment for investors and broker-dealers 105
30. Market-wide Half-Hourly Settlement Programme (MHHS) 109
31. Energy Retail Market Reform – Phase 2 112
32. UK T+1 Settlement: Time enough for implementation, but still no time to waste 115

Financial Risk

33. Reviewing the ECB Pillar 2 Requirements methodology 118
34. OSFI outlook: Credit and liquidity risk 122
35. Dynamic General Insurance Stress Test (DyGIST) 124

Click on the article name to go to the relevant pages. Click on the "back to contents" link on any page in the article to return to the start of the Contents list.

Welcome to the latest edition of Regulatory Horizon.

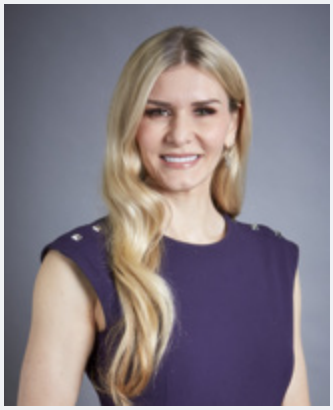
Looking out across the globe, it is clear that regulators' preoccupations are converging around certain key priorities, foremost among them the exponential rise in AI adoption, the integration of ESG, consumer protection and operational resilience, as well as the broader themes integrity, agility and innovation.

Financial crime prevention – not least in the cyber realm – alongside the adoption of advanced data-driven technologies and the governance of data, compliance with sanctions regimes, the rise of fintechs and vulnerabilities arising from third parties also feature on many regulatory agendas.

The UK Financial Conduct Authority's focus on oversight, judgement and accountability is echoed in the EU's efforts to enhance transparency, the drive by the Office of the Superintendent of Financial Institutions (OSFI) to elevate financial integrity in Canada, and the initiatives around APAC aimed at improving investor protections and enhancing operational resilience.

At the same time, regulators and financial services institutions worldwide are keeping a close eye on the reorientation of the US regulatory, enforcement and oversight landscape set in motion by the Trump administration. This 'deregulation' imperative has unquestionably engendered a heightened sense of uncertainty around the trajectory of the world's largest capital market.

At Capco, we remain committed to ensuring our clients across the financial services and energy industries are strongly positioned to map their compliance challenges and navigate both current and future risks. We trust the insights and guidance within the articles that follow will help you in achieving those goals – and to seize strategic opportunities as they arise.



Jamilia Parry
Partner, Global Head of Financial Crime, Risk, Regulation & Finance



1. UK Regulatory Summary

back to contents

The UK's regulatory landscape continues to evolve rapidly, shaped by accelerating AI adoption, ESG integration across energy and financial services, heightened consumer protection, a growing compliance burden from sanction regimes, and increased operational resilience expectations.

The first half of 2025 has seen a significant volume of strategic direction from UK regulators, where the emphasis appears to be a shift from prescriptive compliance to outcome-driven oversight. In March, the FCA published Feedback Statement FS25/2, outlining how it will simplify regulatory requirements in the wake of the Consumer Duty. This is not deregulation – it is a recalibration. Oversight, judgement and accountability are now more important than ever. The PRA's 2025/26 Business Plan reaffirms its focus on promoting the safety and soundness of authorized firms and protecting policyholders. Its 2025-2030 strategy sets four goals: support innovation and growth, prevent financial crime, improve consumer outcomes, and become a smarter regulator. There is also strong emphasis on its secondary objective of supporting competitiveness and growth in the financial sector.

Financial crime

The FCA continues to strengthen anti-money laundering (AML), counter-terrorist financing (CTF), and fraud prevention frameworks. Considering the increase in Authorized Push Payment (APP) fraud, the FCA recommends that firms deploy enhanced Know Your Customer (KYC) processes, sophisticated transaction monitoring systems, and analytics-based tools. The FCA encourages firms to adopt AI and machine learning to detect unusual behavior and improve their financial crime risk management frameworks. The Economic Crime & Corporate Transparency Act is proposed to come into effect during the latter half of 2025, designed to tackle economic crime and improve transparency over corporate entities.

Sanctions

The current sanctions regime is having a significant impact on UK financial services and energy firms, particularly due to its complexity and evolving nature. Firms must navigate a highly fragmented landscape, where sanctions imposed by the UK, EU, US, and other jurisdictions often differ in scope, targets, and how they are enforced. This multi-layered regime creates substantial compliance challenges, as firms must adhere to overlapping and sometimes conflicting rules. The impact on financial institutions is particularly substantial. UK banks and fintechs collectively spend approximately £38.3 billion annually on financial crime compliance. This expenditure encompasses enhanced due diligence, transaction screening, and risk assessment processes, which increase operational costs and legal exposure. Notably, over 65% of suspected sanctions breaches reported to the UK's Office of Financial Sanctions Implementation (OFSI) since February 2022 have originated from financial services firms. [1, 2]

Energy firms, especially those with global supply chains or partnerships in sanctioned regions, face disruptions in trade or restrictions on investment. As sanctions are frequently updated in response to geopolitical developments, their dynamic nature further complicates strategic planning and risk management. The recent cross-government review of sanctions enforcement (May 2025) has acknowledged this complexity and recommended improvements to streamline enforcement, enhance information sharing, and reduce the administrative burden on firms.

Artificial intelligence (AI)

AI continues to gain traction in financial services, from customer service to credit assessment and trading, and multiple consultations on the use of AI (for example, from Ofgem and HOC Treasury Committee) demonstrate increasing regulatory focus. **The Digital Regulation Cooperation Forum (DRCF)**, which includes the FCA, PRA, the Information Commissioner's Office (ICO), and the Competition and Markets Authority (CMA), is leading efforts to create a coordinated regulatory approach to AI. Financial institutions are expected to assess AI risks, such as bias and data quality, particularly where models affect decisions.

1. https://www.herbertsmithfreehills.com/notes/fsrandcorpcrime/2025-posts/sanctions-tracker-%E2%80%93-ofsi-publishes-assessment-of-threats-to-uk-sanctions-compliance-in-financial-services-sector
2. https://www.oxfordeconomics.com/resource/the-true-cost-of-compliance/



> **Firms must navigate a highly-fragmented sanctions landscape - the multi-layered regime creates substantial compliance challenges, as firms must adhere to overlapping and sometimes conflicting rules.**

Shivshanker Subramani
Managing Principal

back to contents

Data governance and reporting

UK regulators increase their expectations about data accuracy, integrity, and availability, especially regarding regulatory reporting. The FCA is advancing digital regulatory reporting (DRR) to automate compliance processes and enhance timeliness. There is also a heightened focus on outsourced data services, with firms expected to maintain robust governance over third-party vendors.

Operational resilience and cybersecurity

Following the full implementation of the UK's Operational Resilience Framework in March 2025, firms are now required to remain within their impact tolerances during severe but plausible disruption scenarios. Since January 2025, the PRA and FCA have also begun exercising new powers over critical third-party service providers (CTPs) such as cloud and data vendors, bringing them within scope for oversight. Both UK regulators also place increasing emphasis on cyber-resilience testing, ICT governance, and the management of systemic risks. The growing regulatory focus was underscored when the Treasury Select Committee summoned nine major UK banks to account for recent IT and operational outages, highlighting the rising pressure to demonstrate resilience across the sector.

In the UK energy sector, Ofgem's RIIO-2 Price Controls set the framework for investment by network companies in infrastructure with a focus on enhancing operational resilience. Furthermore, Ofgem's RIIO-2 Cyber Resilience guidelines help network companies develop robust cybersecurity plans and ensure they meet the evolving cybersecurity needs of the sector.

Energy

The UK's Emissions Trading Scheme (ETS) enters Phase 5 in 2025, with Ofgem expanding its scope and refining carbon pricing mechanisms. UK-based firms with EU trade exposure must also prepare for the **Carbon Border Adjustment Mechanism (CBAM)** and the **EU Deforestation Regulation**, both of which introduce complex traceability and reporting requirements. These measures place new compliance burdens on firms with global supply chains or cross-border operations. Domestically, Energy Retail Market Reform – Phase 2 aims to improve protection for vulnerable customers by introducing targeted measures such as better access to payment plans and faster switching mechanisms to change energy suppliers.

ESG

Sustainability is firmly embedded in the regulatory agenda. The FCA's anti-greenwashing rule, effective as of May 2024, mandates that all sustainability-related claims must be clear, fair, and not misleading. Looking ahead, the **FCA** will consult on the integration of the International Sustainability Standards Board (ISSB) disclosure framework and the introduction of mandatory transition plans for listed companies.

UK energy firms face growing ESG obligations, including adherence to the UK Green Taxonomy, upcoming UK Sustainability Reporting Standards and increasing expectations around climate, nature, and corporate governance disclosures.

Conduct

In 2025/2026, consumer protection – particularly for vulnerable individuals – remains at the heart of the FCA's conduct agenda; the focus on vulnerability is also reflected in the energy sector, where Ofgem recently published its own Consumer Vulnerability Strategy. Following the rollout of the Consumer Duty, firms must demonstrate how they deliver fair value, prevent foreseeable harm, and support good consumer outcomes. The **Pure Protection Market Study** has also highlighted concerns over commission structures and sales practices in the insurance market, prompting calls for reforms to better serve consumers.

More broadly in insurance, the FCA plans to strip outdated or duplicated requirements from its insurance rulebook, having asked firms what improvements it could make. The regulator is also proposing to create a new definition to identify large commercial insurance customers who should not be captured by its conduct rules. This should ease the burden on firms insuring larger businesses, while protecting smaller commercial customers.

Conclusion

As regulation across the UK's financial and energy markets grows more sophisticated, emphasizing greater transparency and more rigorous reporting obligations, firms are increasingly reliant on advanced data-driven technologies. This demands an outcomes-focused approach and firms should focus on the following key priorities:

- Enhancing AML / KYC processes and smart financial crime monitoring tools
- Implementing ethical AI use frameworks
- Ensuring strong data governance, reporting automation, and oversight of third-party providers
- Strengthening operational resilience and cybersecurity
- Preparing for ESG disclosure reforms and ensuring anti-greenwashing compliance
- Prioritizing consumer protection and redress efficiency, with a focus on vulnerable customers.





2. US Regulatory Summary

back to contents

President Trump took office on January 20, 2025, and immediately began reorienting the regulatory, enforcement, and oversight landscape for financial institutions operating within the US and across the globe. The Trump Administration moved quickly to reverse the policies of the Biden Administration but also put a halt to enforcement actions, litigations, and investigations under the purview of the various prudential and consumer regulators.

One of the most powerful policy tools President Trump has used since the beginning of his administration was the Executive Order (EO). He has signed more than 200 EOs, and many of these have been used to take direct control of all financial services policies and regulations. These EOs have taken a number of forms, including using a "Deregulatory Initiative Order" for his administration to conduct a review of all regulations and potentially rescind "unlawful regulations and regulations that undermine the national interest," as well as an EO to directly supervise and control "independent regulatory agencies," such as the US Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), and the Consumer Financial Protection Bureau (CFPB).

Actions taken by President Trump, and the various policy and regulatory responses to them, are illuminating a number of key themes that are expected to play out over the next four years, including those on "deregulation," the role of the US Congress, state-by-state enforcement, and efforts by the governments in Canada, Mexico, the United Kingdom (UK) and across the European Union (EU).

The first trend is the Trump Administration's focus on deregulation. President Trump has the authority to take a number of actions focused on deregulation, including rejecting final rules issued under the Biden Administration under the Congressional Review Act (CRA), issuing Executive Orders (EOs) to freeze or withdraw regulations, and modify existing rules under the Administrative Procedure Act (APA) (e.g., CRA, M&A), and simply not enforce current laws or regulation. There has been only one significant change to consumer protection laws since January 20, 2025, with the passage of the joint resolutions of disapproval overturning the CFPB's final rule to impose certain limits on overdraft fees (overdraft rule).

As financial institutions examine whether to deprioritize compliance plans for certain regulations and anticipate a new approach to specific policies, they should balance the President's communication of support for deregulation with the potential for the more populist elements of the party to maintain particular policies. The Trump Administration and the Department of Government Efficiency (DOGE) are also redefining the current structure and staffing models for the federal agencies that regulate and supervise financial institutions.

The second trend that financial institutions are closely following is the Trump Administration's coordination with the US Senate and the US House of Representatives on the President's policy priorities and how those are enacted through the CRA and budget reconciliation. These committees have identified a number of policy areas where there is agreement with the President and the Congress to deregulate, including Basel III, CAMELS ratings, the Corporate Transparency Act (CTA), digital assets, and housing policy.



President Trump has signed more than 200 Executive Orders, many of which have been used to take direct control of financial services regulations.

The third trend is laws, regulations, and litigation in states where Democrats hold the governorship and majority in the state legislatures and serve as a counterweight to the Trump Administration's financial services policy priorities. Several Democratic state governors formed the Governors Safeguarding Democracy to protect "state-level institutions of democracy." Several states have discussed coordinating investigations, enforcement, litigation, opposition to regulations, and preparing multistate legal challenges. With concerns for freezing supervision, litigation, examinations, and enforcement by the CFPB, states, state banking and securities regulators, and state attorneys general are expected to initiate consumer protection investigations and penalties for consumer protection and private enforcement. As of May 1, 2025, the Trump Administration has been hit with over 200 lawsuits to stop or limit the President's enforcement and public policy changes.

The fourth trend expected to play out over the next several years is efforts by governments in Canada, the EU, and the UK to address regulation and enforcement where there is a public policy and regulatory divergence (e.g., AI, Basel III, climate change, ESG, etc.) and disagreements on international standards (e.g., Financial Stability Board (FSB), Bank for International Settlements (BIS), etc.).

This trend is increasingly creating challenges for financial institutions operating in the US with a global operational footprint, especially those in the UK and EU. The US does not have similar legislative or principal-based frameworks for regulating crypto assets, AI, sustainable finance, and climate change (e.g., EU AI Act, MiCA, SFDR, CA Bank Act, etc.). These global institutions face growing complexity and further pressures to ensure global and regional compliance and risk monitoring across divergent regulatory standards and must decide whether to apply the highest standards enterprise-wide or tailor their approach on a country-by-country basis. These institutions should continue to monitor and address regulation and enforcement issues and, at the same time, respond to geopolitical events and government actions that might affect a financial institution's risk profile. Geopolitical risk management has become an operational imperative.

These trends and the following priority areas for the Trump Administration in 2025-2026 will be significant in considering how firms must monitor and implement changes to laws, regulations, guidance, and enforcement actions at the international, national and state levels. The increased focus on state-by-state oversight is also introducing increased complexity for compliance and risk management for assessing emerging issues or potential threats.

Supervision and examination

The CFPB saw immediate changes to its staffing levels and was required to halt all activities, including requiring employees to work remotely and stopping all supervision. The CFPB is shifting its previous focus on both banks and non-banks to prioritize supervision of primarily depository institutions, reducing the overall number of exams by 50% and potentially amending its Sec. 1033 and Sec. 1071 rulemakings.

The Office of the Comptroller of the Currency (OCC) has also seen several changes to the organization, including reducing its staffing levels and combining its midsize and community bank supervision and the large bank supervision functions. The Acting Comptroller, Rodney Hood, withdrew from the Network of Central Banks and Supervisors for Greening the Financial System and deprioritized climate change risk management, ceased examinations for reputation risk, and clarified its position for oversight for banks engaging in crypto-asset custody and stablecoin activities through issuing new guidance and rescinding previous guidance that limited financial institutions from providing financial services and products to digital asset companies. The OCC has prioritized four areas it is expected to focus on next year: reducing regulatory burden, promoting financial inclusion, embracing fintech, and expanding responsible banking in the digital asset area.

The Federal Deposit Insurance Corporation (FDIC) and the Board of Governors of the Federal Reserve System (Federal Reserve) took similar approaches for the reprioritization away from climate change risk management. They withdrew from the Network of Central Banks and Supervisors for Greening the Financial System (NGFS). The OCC, FDIC, and Federal Reserve have also recently revoked previous supervisory guidance concerning crypto-asset activities, signaling a shift in their approach to overseeing banks that are planning to or currently engaging in digital asset services. As the heads of these agencies are confirmed to lead each organization, there are likely to be more changes.



M&A

With President Trump's election, it has been widely expected that his economic, tax, and deregulation agenda would lend itself to a better M&A environment. The significant fluctuations in tariffs had initially slowed down M&A amongst the largest banks in the US, but with community banks, there has been an appetite for M&A amongst similarly sized and situated institutions.

The OCC issued an Interim Final Rule on Bank Mergers and rescinded the 2024 policy statement under the Bank Merger Act. The FDIC rescinded the agency's 2024 Statement of Policy on bank merger transactions, which reverses the Biden Administration's policies on bank merger reviews. These policy changes are expected to drive additional M&As in 2025 and expedite and ease the process for these transactions to receive approval from their regulator(s) as was seen under the approval of Capital One to acquire Discover Bank.

Digital assets

The administration's support for crypto assets businesses is a hot topic in the US. The Trump Administration has consistently stated that it will support efforts to ease the regulatory burden and oversight process to allow the digital asset industry access to custody services, investment products and services, and intermediated payments exchanges. Prudential, securities, and commodity regulators have held roundtables, announced task forces, and appointed key members of the leadership teams with a background in digital assets.

The President's EO on Strengthening American Leadership in Digital Finance Technology points to a coordinated effort to ensure a regulatory and economic framework supports the US leadership in digital assets and that "digital asset industry plays a crucial role in innovation and economic development in the United States, as well as our Nation's international leadership." Congress has also moved quickly to provide legislative support. It is considering multiple legislative proposals, including the Stablecoin Transparency and Accountability for a Better Ledger Economy (STABLE) Act of 2025, Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act, and Anti-CBDC Surveillance State Act.

Bank-fintech partnerships

Financial institutions increasingly rely upon third parties to provide critical products and services to their customers, banking-as-a-service (BaaS), or bank-fintech partners. The Biden Administration closely scrutinized these relationships through the examination process and under Interagency Guidance on Third-Party Relationships issued by the Federal Reserve, the FDIC, and the OCC. The Trump Administration, while continuing to monitor third-party risks to financial institutions and the banking system, is taking a more supportive role in enabling these partnerships.

The Acting Comptroller of the OCC recently identified that these partnerships are essential to banks offering innovative products and services to their customers. The FDIC and Federal Reserve have also taken steps to better engage with banks to understand the risks from these partnerships and what steps need to be taken to mitigate risks while allowing banks to be innovative. The House Financial Services Committee has recommended that "the agencies should revise the existing guidance or issue new guidance that provides greater clarity to financial institutions and their third-party vendors." The risks from third-party relationships will continue whether or not there is formal guidance. Financial institutions will need to continue to manage and prioritize safety, soundness, and reputational risks, regardless of the administration's optimistic view of their partnerships.

Artificial intelligence (AI) regulation

Immediately upon taking office, President Trump issued an Executive Order, "Removing Barriers to American Leadership in Artificial Intelligence," requiring his administration to review all policies and regulations issued under the Biden Administration's EO on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." President Trump's EO also requires his administration to develop and submit to the President an action plan on AI within 180 days. This action plan will provide financial institutions with expectations regarding the development of regulations and guidance under each agency's purview.

With the federal government rescinding nearly all of the Biden Administration's policies and guidance on AI, states have begun aggressively passing legislation for how businesses operating in their respective states should manage and mitigate risks for AI, including AI-generated content, disclosures on the use of AI, opt-out of the processing of their data, and the use of AI in making credit decisions. There are currently over 500 bills on AI that state legislators are passing. Financial institutions must monitor these bills and ensure that those that impact the delivery of products and services, or their critical vendors, comply with these laws.

Conclusion

Changes to financial services regulations, supervision, and enforcement are happening at pace. While there is the expectation that deregulation may be a positive for financial institutions as more business-friendly policies are implemented, the current environment is creating business challenges that require a surveillance and risk management framework that can respond to these challenges.

What is becoming more certain is that President Trump and his administration will continue to take a US-centric approach to regulation and enforcement that will allow US-based financial institutions to better compete in domestic and international markets. The challenge for global banks, operating primarily in the EU, UK, and Asia, is the balance of operating in domestic markets with higher governing standards and additional regulatory scrutiny, while at the same time ensuring they are positioned for profitability and economic growth in a rapidly changing geopolitical environment.





3. Canada Regulatory Summary

back to contents

Canada's financial regulatory environment is entering a period of rapid change in 2025-2026, marked by intensified oversight and new expectations for financial institutions. The Office of the Superintendent of Financial Institutions (OSFI) has reshuffled its risk priorities, elevating threats such as cybercrime, financial integrity, and third-party vulnerabilities to the top of its Annual Risk Outlook. Interest rate and liquidity risks remain key focus areas, while credit risks, ranging from corporate debt to consumer and commercial real estate exposures are under heightened scrutiny.

At the same time, trade disruptions are roiling international markets, and 2025/2026 promises to be a time of uncertainty and reset expectations. In Canada, the surprise reelection of a Liberal government has left the country's policy and governance agenda similarly unclear.

OSFI's Annual Risk Outlook for 2025-2026 outlines four priority risk areas that will shape supervisory expectations and regulatory action in the year ahead. These priorities signal where financial institutions should direct their attention, and they provide a roadmap for upcoming OSFI guidance, oversight, and enforcement efforts:

1. Integrity and security risk

2. Wholesale credit risk

3. Funding and liquidity risk

4. Real estate secured lending (RESL) and mortgage risk

Integrity and security risk

Heightened geopolitical tensions, non-state actors, and the rise of AI are driving increased exploitation of cyber vulnerabilities, money laundering potential, fraud, ransomware, scams, and even foreign interference in the financial and media systems. These risks are further amplified by complex third-party and n-party relationships. OSFI is recommending that organizations invest in strengthening controls and response frameworks across AML, cybersecurity, and third-party risk management (TPRM).

Wholesale credit risk

OSFI continues to flag risks in corporate and commercial lending. Although recent interest rate cuts have eased some pressure, businesses remain strained by elevated borrowing and debt servicing costs. In commercial real estate in particular, the lingering effects of remote work continue to manifest in rising office vacancies and falling property values especially in Tier 2 and Tier 3 properties. Loan loss provisions and robust stress testing will be critical. Broader uncertainty persists, driven by the unknown effects of US tariffs on the Canadian economy, the potential for reduced interprovincial trade barriers, and Chinese goods being redirected to non-US markets.

Wholesale credit risk in Canada remains elevated as corporate and commercial borrowers face persistent macro-economic uncertainties, high debt servicing costs and weakening consumer demand.

Funding and liquidity risk

Despite a strong environment for depositors and lower interest rates, OSFI continues to highlight liquidity risk as a growing concern. Volatile markets, international uncertainty, and consumer confidence challenges could all lead to funding pressures across the market. The introduction of real-time payments will increase the importance of effective intraday liquidity monitoring. OSFI plans to adopt a more structured approach to liquidity supervision and will publish a discussion paper on the Internal Liquidity Adequacy Assessment Process (ILAAP). This will require participants to implement holistic liquidity plans and develop strategic risk management and mitigation frameworks.

Real estate secured lending (RESL) and residential mortgage risk

Although interest rates declined significantly in 2024, roughly 36% of residential mortgages originated during the ultra-low-rate environment of 2020-2021 are due to renew at much higher rates over the next 12 months. Combined with a weakening economy, these factors are expected to place significant strain on households with high loan-to-income ratios and overleveraged buyers. A soft housing market further reduces homeowners' flexibility to adjust. OSFI has responded proactively, tightening underwriting standards under Guideline B-20.

Other key regulatory developments

Anti-money laundering and counter-terrorist financing

Canada is strengthening its AML/ATF regime with expanded regulations effective April 1, 2025. Sectors like payday lenders and factoring firms must now comply with PCMLTFA obligations, including customer due diligence and suspicious transaction reporting. Banks also face greater obligations when dealing with these entities. Additional measures include mandatory discrepancy reporting to the federal beneficial ownership registry (beginning October 2025), enhanced interbank information sharing, and required reporting of suspected sanctions evasion. These changes will require banks to upgrade transaction monitoring, train staff, and bolster compliance programs. FINTRAC is also adopting a more aggressive enforcement stance, with increased penalties following recent high-profile lapses.

Crypto assets

Amid renewed interest in crypto assets and rising Bitcoin prices, the Canadian Securities Administrators (CSA) have updated their guidance for institutions engaged in crypto activities. New measures include

The economic integrity, public safety, and global reputation of Canada are currently under threat; Canadian regulators have flagged weak financial crime security enforcement and ownership transparency. Recent reforms changing the way Financial Institutions operate include mandatory reporting, stricter crypto regulations, and heightened penalties.



mandatory registration, tighter custody requirements, product limitations, and a ban on leverage. These "guardrails" aim to support a more stable, regulated crypto ecosystem and form part of a broader regulatory framework for trading platforms.

Payments modernization

Despite repeated delays, Payments Canada is expected to launch Real-Time Rails (RTR), a new 24/7 instant payments system, in late 2025. The platform will use ISO 20022 messaging standards, enabling richer data flows and innovation across the payments ecosystem. However, RTR also introduces greater fraud risk due to the speed and irrevocability of transactions. Although Payments Canada is developing a parallel fraud detection system, faster payments will still require banks to enhance oversight to mitigate growing threats such as authorized push payment scams.

Data privacy and protection

The recent proroguing of Parliament has effectively ended Bill C-27, which would have introduced the Consumer Privacy Protection Act (CPPA) and the Artificial Intelligence and Data Act (AIDA). These would have modernized Canada's privacy framework and introduced new rules for AI use in financial services. While legislative progress is delayed, privacy reform and AI regulation remain imminent. Banks should prepare for stricter controls on consumer data and possible unwinding of certain AI use cases depending on final rulemaking.

Looking forward

While the demise of C-27 has delayed a federal response to AI, the associated risks and opportunities remain central to regulatory conversations. Financial institutions are encouraged to act now by developing enterprise AI strategies, appointing chief data & AI officers, strengthening encryption and data governance, and improving model risk management with an emphasis on explainability in AI-driven decisions.

Open banking was briefly addressed in the previous Liberal government's economic statement under the term "Consumer-centric banking". While Canada has been slow to adopt a federal open banking policy, the implementation of Section 1033 of the Dodd-Frank Act in the US makes a similar regulatory shift increasingly likely in Canada. Banks should begin investing in API and data infrastructure now and start building a roadmap for open banking to ensure future readiness and monetization.

Conclusion

2025-2026 will test financial institutions in demonstrating agility and foresight. Those that treat regulatory compliance as a baseline, not the end goal, and strive to go further by strengthening operational resilience, fostering a culture of integrity, and aligning innovation with regulatory expectations, will be better positioned to navigate risks and seize strategic opportunities. By establishing a clear direction, compliance and risk leaders can guide their organizations' policy to thrive in a rapidly evolving environment.





4. EU Regulatory Summary

back to contents

Over the next 12-18 months, the European Union (EU) will introduce significant regulatory changes across financial services and energy sectors. These changes aim to enhance transparency and resilience, addressing emerging risks and opportunities, while also enabling easier market entry for fintechs. They include enhanced financial crime prevention, regulation of AI, and data governance. These are on top of recent changes that firms are continuing to embed, such as Digital Operational Resilience (DORA). Firms must continue to adapt to these regulations to ensure compliance and leverage potential opportunities, as well as having an eye on upcoming regulations and their potential impact.

Financial crime

The EU is set to introduce stricter measures to combat financial crime through a new body, the Anti-Money Laundering Authority (AMLA), which is aimed at strengthening efforts to combat money laundering and terrorist financing. It is a decentralized EU agency that will coordinate national authorities to ensure the consistent and harmonized application of EU rules, creating a cohesive framework to combat financial crime. Its aim is to transform anti-money laundering and countering the finance of terrorism (AML/CFT) supervision in the EU and enhance cooperation amongst financial intelligence units (FIUs). AMLA will provide enhanced cross-border coordination, focus on high-risk entities, improved data management and technology use, and stronger enforcement. The establishment of a centralized AML/CFT database and the use of advanced IT tools will significantly enhance data analysis capabilities, allowing for more proactive and data-driven supervision and information sharing among FIUs.

The upcoming sixth Anti-Money Laundering Directive (AMLD VI) must be transposed into national law by July 2027.

The upcoming sixth Anti-Money Laundering Directive (AMLD VI), which must be transposed into national law by July 2027, further strengthens measures to combat money laundering and terrorist financing – it will mandate more rigorous checks on transactions and beneficial ownership transparency. These are a few examples of changes that will be coming with AMLD VI:

1) Reporting obligations for all transactions of high-value goods (motor vehicles > € 250,000, boats and airplanes > € 7.5 million) in connection with financial services.

2) The AMLD VI sets out guidelines on the conditions under which third parties can be utilized and outsourcing restrictions and the respective tasks and responsibilities of the parties involved

3) The legislation also includes stricter monitoring rules for particularly wealthy individuals, an EU-wide cap of €10,000 on cash payments, as well as measures to ensure compliance with targeted financial sanctions and to prevent the evasion of sanctions.

Gen AI

The EU's AI Act, which enters into force in August 2025, is set to become one of the most stringent and comprehensive regulatory frameworks worldwide, explicitly reflecting OECD principles through a clearly delineated, risk-based approach. It classifies AI applications into categories ranging from unacceptable and high-risk to minimal risk, imposing heavy compliance obligations on high-risk systems, including many critical to financial services, such as credit scoring, investment advisory, and risk management. Transparency, explainability, and robustness are mandated to safeguard consumer rights and ensure financial stability, aiming to maintain consumer trust and prevent systemic disruptions arising from algorithmic errors or biases.



ESG

The European Commission has adopted a package of proposals ("ESG Omnibus Directive") designed to simplify rules, boost competitiveness and unlock additional investment capacity. They have approved significant changes to the Corporate Sustainability Reporting Directive (CSRD) and the Corporate Sustainability Due Diligence Directive (CSDDD).

The proposals will reduce complexity of EU requirements for all businesses, particularly SMEs and small mid-caps (SMCs). They also focus the regulatory framework on the largest companies that are likely to have a bigger impact on the climate and the environment. The transposition deadline is delayed by one year (to July 26, 2027) and the first deadline for the largest companies to comply with sustainability due diligence requirements is also delayed (to July 26, 2028). Additionally, a guideline defining ESG scenario analysis and the requirement to create mid- and long-term transition plans for financial institutions by January 2026 is expected to be signed off shortly.

Beyond adhering to regulation, more and more banks are starting to leverage the insights they have gained / are gaining from the ESG data and use them to be integrated within existing risk management processes and tools.

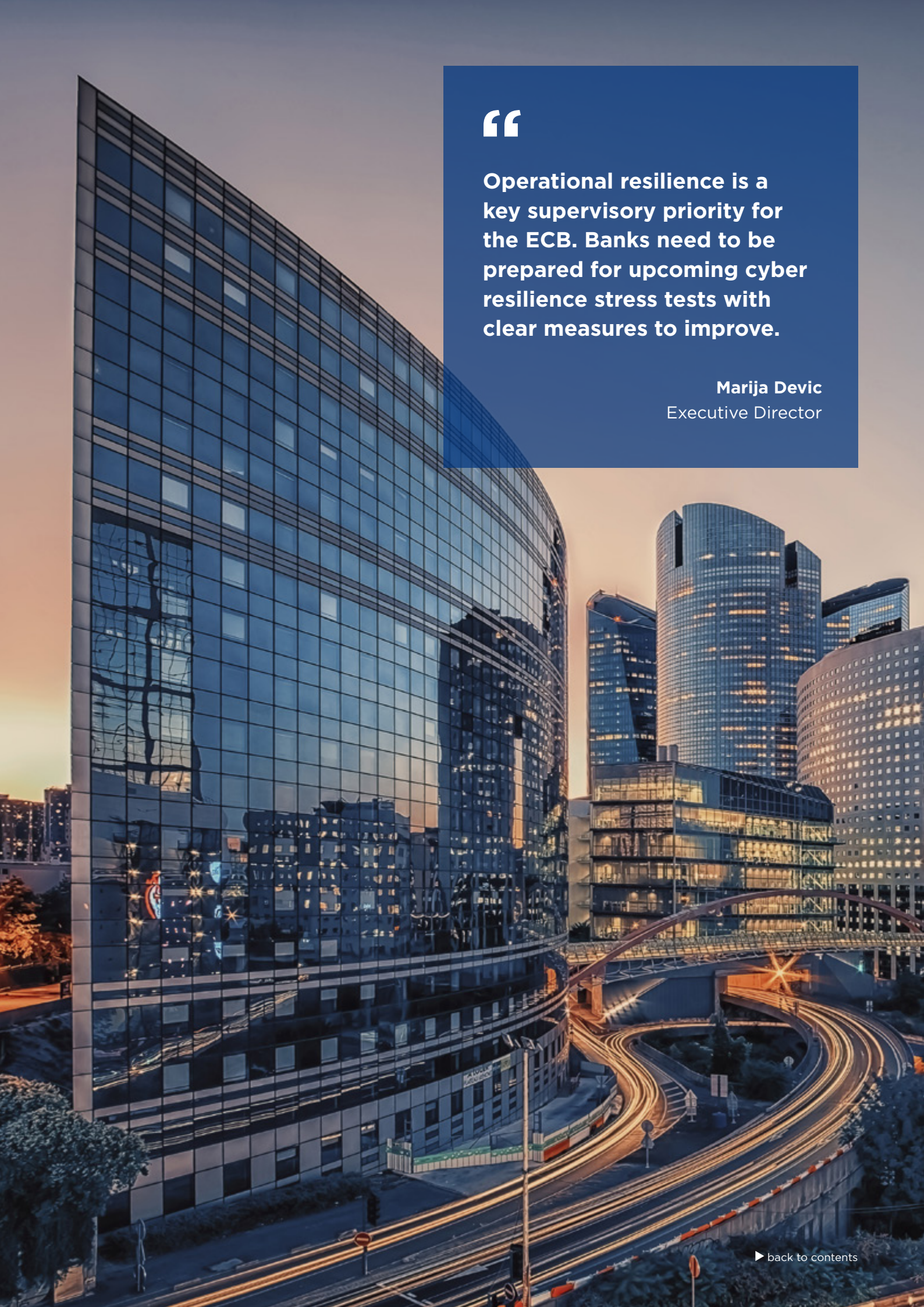
Operational resilience and cybersecurity

Operational resilience and cybersecurity are critical areas of focus: the EU's Digital Operational Resilience Act (DORA) entered into force on January 16, 2023, and its provisions were fully applied as of January 17, 2025, requiring firms to strengthen cyber defenses, conduct regular risk assessments, and establish comprehensive incident response plans. Financial entities are now expected to be fully compliant with DORA requirements.

ECB has stated in its supervisory priorities for 2025-27 operational resilience as key on their working agenda. The ECB expectation is that banks should be compliant with the legal requirements stemming from DORA. Deficiencies in operational resilience frameworks, as regards IT outsourcing and IT security/cyber risks, will be penalized via SREP and OSIs. Banks need to be prepared for upcoming cyber resilience stress tests with clear measures to improve, e.g., business continuity frameworks, incident response planning, back-up security, and management of third-party providers.

Capital markets and digital assets compliance

Transaction reporting and transparency will be enhanced through the reviewed Markets in Financial Instruments Directive (MiFID II) and Regulation (MiFIR). These regulations will improve market transparency and efficiency, particularly in over-the-counter (OTC) markets. The transposition deadline for EU member states to implement the revised framework is September 2025. In April, the European Securities & Markets Authority (ESMA) published draft regulatory technical standards and final guidelines on liquidity management tools, as required under the revised Alternative Investment Fund Managers' Directive (AIFMD II) – the legislation is due to take effect in Q2 2026, two years after AIFMD entered into force. The EU Commission is currently examining simplifications to the Retail Investment Strategy (RIS) proposal with possible effects on various existing legal provisions, such as MiFID II, IDD, PRIIPs, ICITS, AIFMD, and PEPP, which must be taken into account in the regulatory monitoring process for upcoming changes with potential impacts on processes, (ex-ante/ex-post) reporting and transparency requirements, data and IT, as well as on policies.



> **Operational resilience is a key supervisory priority for the ECB. Banks need to be prepared for upcoming cyber resilience stress tests with clear measures to improve.**
>
> **Marija Devic**
> Executive Director

▶ back to contents

Data governance and reporting

The EU's **Data Act** is a law designed to enhance the EU's data economy and to create a competitive data market by making data (in particular industrial data) more accessible and usable, boosting its economic value, and encouraging data-driven innovation and increasing data availability. It covers data-sharing between businesses, consumers, and governments.

The majority of the EU Data Act's Provisions will apply from September 12, 2025.

The new rules will encourage the use of data and ensure it is shared, stored, and processed in full respect of European rules. For businesses, this means changes in how they handle and share data, with potential implications for both those providing access to data and those seeking access. Businesses will need to ensure products and services enable data sharing by default, make data readily available, and comply with data protection principles. There are a number of implications, including, potentially, product re-design and increased costs.

The majority of the EU Data Act's provisions will apply from September 12, 2025, as this is the end of the 20-month transition period.

Energy

The European Commission is considering changes to EU energy laws as part of its next package of proposals to cut the regulatory burden for struggling industries and to help them compete against China and the United States, where regulation is being rolled back. The intent is to remove layers of bureaucracy, similar to the omnibus simplification rules recently published on sustainability.

Payments and data access

Building upon the Payment Services Directive 2 (PSD2), the EU published the consultation paper for the Financial Data Access regulation (FIDA) to level the playing field and enable market entry for fintech and third-party providers. While currently not binding, based on previous experience with overarching EU regulations, we do not expect fundamental changes to the regulation. Financial institutions will need to upgrade existing systems to facilitate safe and efficient data sharing access across the financial sector, while complying with the added consumer rights requirements.

Conclusion

The forthcoming regulatory changes in the EU across financial services and energy sectors will require firms to adapt their strategies, invest in compliance technologies, and enhance their operational practices. The increasing unpredictability of the global economy means that firms must remain agile to respond to regulatory adjustments and simplifications, as they occur.





5. APAC Regulatory Summary

back to contents

Several APAC regulators have outlined priorities for 2025.

In 2025 and beyond, APAC regulatory landscapes will increasingly emphasize ESG compliance, with standardized reporting frameworks and heightened scrutiny on sustainability practices. Data protection laws will tighten, aligning more closely with global standards. Operational resilience and cybersecurity regulations will require financial institutions to enhance their defenses against emerging threats. Stricter anti-money laundering (AML) measures will evolve, leveraging technology for better monitoring. Additionally, guidelines for GenAI will focus on ethical usage in financial services. Market regulations will aim to boost transparency and investor protection, creating a more robust and resilient financial ecosystem across the region.

1. ESG

APAC regulators are increasingly focused on green finance and anti-greenwashing measures, with new climate-related risk rules coming into force, requiring better assurance and board-level ESG oversight. Sustainability and climate risk disclosures are becoming mandatory or more detailed in most markets.

As of December 2024, 30 jurisdictions have adopted or are in the process of adopting the **International Sustainability Standards Board (ISSB) standards**, under the **IFRS**. Statuses of APAC markets are summarized below as of early 2025:

Status	Market
Markets committed to having ISSB-aligned climate-related disclosures	**Hong Kong**, **Singapore**, **Australia**, **Malaysia** and **Taiwan**
Markets moving towards mandating ISSB-aligned or ISSB-referenced climate-related disclosures	**China**, **South Korea** and **India**

2. Data protection and privacy

APAC regulators have recently been actively promoting and upgrading their legal frameworks to emphasize data protection and privacy to safeguard personal data, build consumer trust, and facilitate cross-border trade.

Data laws are tightening (especially in China and Taiwan), with stricter requirements for data mapping, classification, and breach notification. APAC markets are aligning privacy rules with global standards, making cross-border compliance more challenging but also more predictable.

In the first half of 2025, several APAC markets announced or enacted notable data protection regulations:

India introduced the Digital Personal Data Protection Act and the Draft Rules, emphasizing data security and imposing restrictions on cross-border data transfers.

Malaysia implemented key amendments to the Personal Data Protection Act, mandating Data Protection Officer appointments and introducing stricter penalties for breaches.

Singapore Monetary Authority reinforced compliance with the Personal Data Protection Act, focusing on responsible data management by financial institutions.

South Korea enacted amendments to the Credit Information Act, enhancing MyData services, and revised the Personal Information Protection Act to strengthen obligations for foreign entities.

Thailand issued guidelines from the Personal Data Protection Committee to align with GDPR, promoting data subject rights and compliance measures for businesses.

These developments reflect a regional trend towards tighter data protection and privacy standards.



3. Operational resilience and cyber

Cyber and operational resilience are now front-and-center, with regular drills, third-party risk management, and stricter incident reporting expected. APAC regulators want firms to prove they can handle disruptions and cyberattacks, especially as threats grow more complex. They are mandating robust third-party management frameworks and enhancing cybersecurity protocols to safeguard against evolving threats.

Across APAC markets, regulators are set to introduce stricter operational resilience requirements in 2025, including more rigorous incident response, business continuity, and disaster recovery planning expectations. Cyber-risk management will be a key focus, with a push for robust controls, regular vulnerability assessments, and vendor risk management. Enhanced scrutiny of emerging technologies will also aim to mitigate potential operational risks. Key changes include more regular cyber-threat intelligence sharing, multi-factor authentication, scenario-based incident response exercises, and integrating cyber risk into overall risk frameworks.

4. Financial crime

AML/CFT remains a top priority across APAC markets, with regulators demanding stronger controls, especially for digital assets and cross-border transactions. Financial crime risk is rising due to tech advances and geopolitical tensions, so firms need to invest in smarter compliance and monitoring.

Regulators in the Asia-Pacific region have significantly expanded anti-money laundering (AML) and counter-terrorist financing (CTF) requirements for financial institutions. New rules mandate enhanced customer due diligence, with firms required to screen clients against expanded sanctions lists and utilize advanced transaction monitoring. Firms must also appoint dedicated AML/CTF compliance officers and implement comprehensive training programs. Penalties for non-compliance have increased, with regulators empowered to levy heavy fines and even revoke business licenses.

In Hong Kong, the Securities and Futures Commission (SFC) is strengthening AML/CFT regulations for licensed corporations, virtual asset service providers, and associated entities. Recent circulars emphasize enhanced due diligence, risk-based approaches, and stricter controls to combat money laundering and terrorist financing. The measures, issued between January and May 2025, respond to Financial Action Task Force (FATF) and United Nations (UN) sanctions.

In Japan, the Financial Services Agency (FSA) published a discussion paper on validating the effectiveness of AML/CFT frameworks, focusing on practical issues and dialogue, issued on March 31, 2025.

All these changes aim to bolster AML/CFT regimes.

5. AI/Gen AI

APAC markets are moving from voluntary AI guidelines to more binding, risk-based regulations: South Korea will be implementing its new AI Basic Act, Taiwan, Japan and India are drafting new laws, while others, like Singapore and Hong Kong, are leveraging existing privacy/data laws. There is a big push for systems testing, monitoring, and ethical AI use, with many markets eyeing EU-style standards for future alignment.

In the first half of 2025, APAC markets are witnessing significant regulatory changes regarding AI and generative AI (Gen AI). Key themes include enhanced transparency requirements for AI systems, necessitating clear disclosure of data sources and decision-making processes. Regulators are prioritizing data sovereignty, mandating local data storage to bolster privacy and security. Additionally, sector-specific regulations are emerging, particularly in finance, to address ethical considerations and risk management. Compliance frameworks are evolving to tackle cross-border challenges, ensuring that tech firms can navigate diverse regulatory landscapes while promoting responsible AI use to safeguard consumer interests and market stability.



6. Market regulations and guidelines

In early 2025, APAC regulatory updates focused on enhancing trading efficiency, investor protection, and adapting to technological advancements.

India expanded the optional T+0 settlement cycle for equity markets and leveraged digital infrastructure to reduce unclaimed assets. India implemented new regulations for digital asset exchanges, including mandatory KYC and reporting requirements.

APAC is moving towards stricter, more harmonised rules on ESG, cyber and data.

Singapore updated its variable capital company framework to attract more fund managers. Hong Kong updated guidelines for IPO subscriptions and virtual asset funds. Hong Kong and Singapore have begun looking into the technological requirements for a move to T+1 settlement.

Regulators in Hong Kong and South Korea introduced measures to strengthen oversight of specific financial products and trading activities, such as accumulators and short selling. Authorities also implemented guidelines to promote market integrity, transparency, and confidentiality around activities like market soundings.

All these changes reflect a regional effort to modernize capital markets, mitigate risks, and build investor confidence.

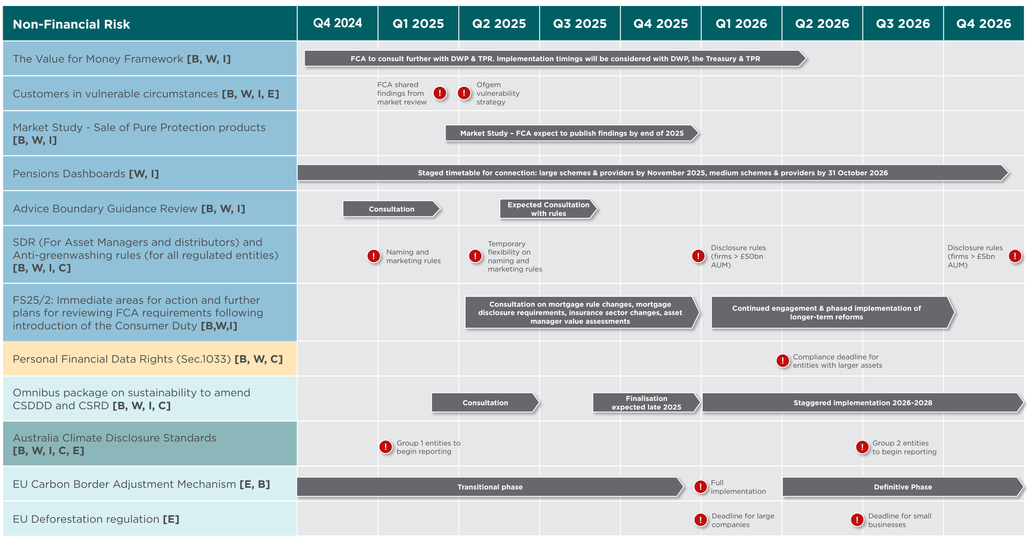
Overall, APAC's regulatory landscape is getting more complex and fragmented, with local nuances, but a shared focus on balancing growth, innovation, and systemic safety. In short, APAC is moving toward stricter, more harmonized ESG, cyber, and data rules, while also fostering innovation in AI and digital assets, although the pace and focus vary by market.

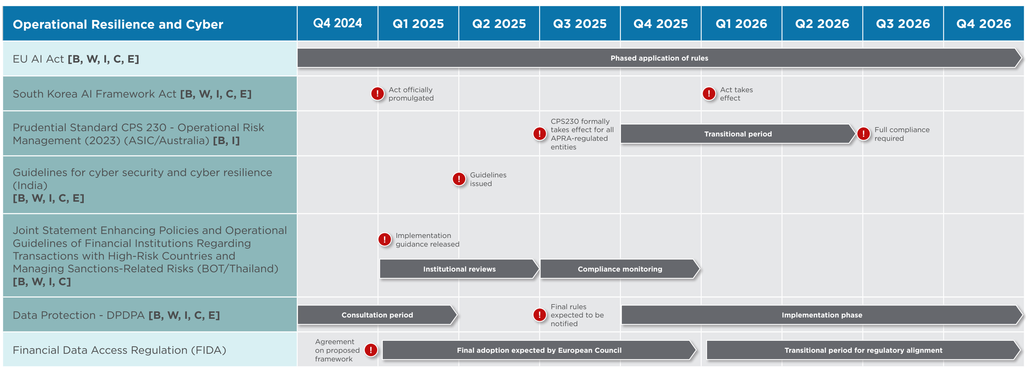


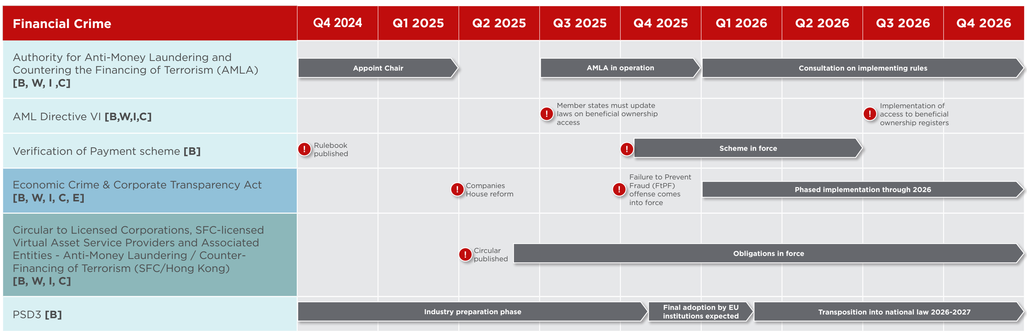
CAPCO
a wipro company

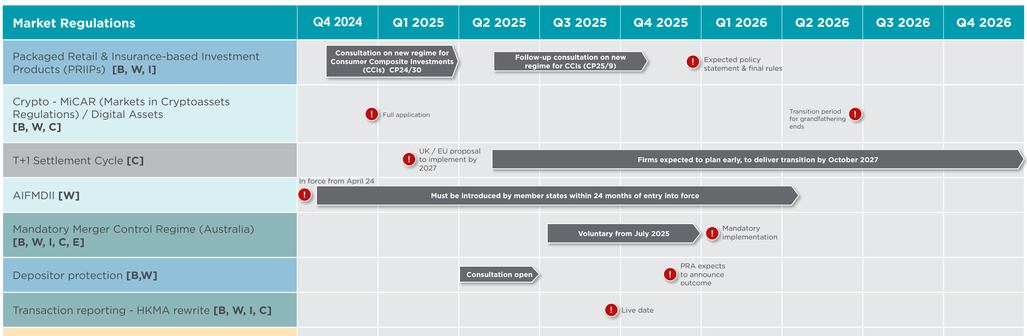
6. Regulatory Heatmap

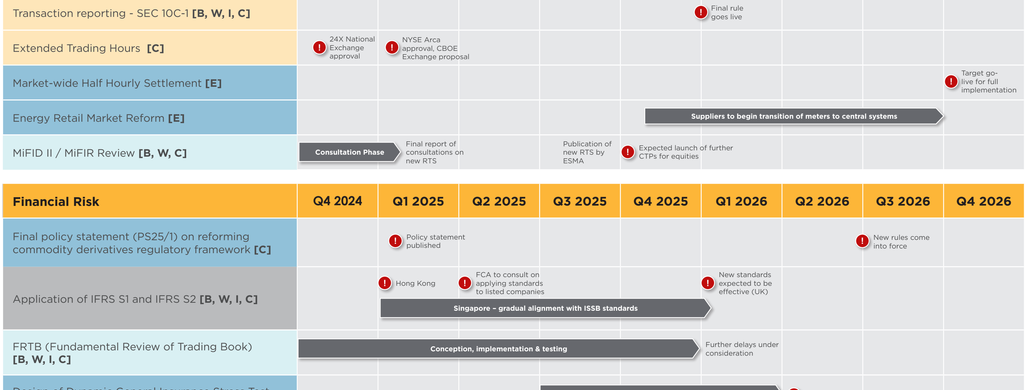
Upcoming key requirements for financial institutions & Energy firms











Keys Publication or adoption | UK | US/Canada | EU | APAC | Global

B - Banking and Payments
I - Insurance
W - Wealth + Asset Management
C - Capital Markets
E - Energy

▶ back to contents



Non-Financial Risk

▶ back to contents

7. The 2025 Omnibus package – EU push for simpler, smarter sustainability rules

On March 27, 2025, the European Commission released a draft Omnibus Directive and Regulation as part of its Sustainable Finance Framework Simplification Package. Currently open for consultation (until June 28, 2025), this is not the final guidance, but a policy proposition aimed at streamlining some of the EU's most ambitious ESG legislation:

- Corporate Sustainability Reporting Directive (CSRD)
- Corporate Sustainability Due Diligence Directive (CS3D)
- EU Taxonomy Regulation.

Why was Omnibus introduced?

The Omnibus is a direct response to widespread market concerns about the complexity and overlap of the EU's sustainability rules. Strong stakeholder feedback from financial institutions and corporates called for greater clarity, coherence, and proportionality across the EU's sustainability rules. The goal is not to lower ambition, but to make ESG compliance more practical and efficient, especially for SMEs and firms operating across multiple regulatory frameworks.

The Omnibus package proposes targeted legislative amendments, focusing on consistency, proportionality, and simplification. Its key proposals include:

- **Reduce duplication and harmonize and clarify definitions and concepts** between CSRD, CS3D, and Taxonomy obligations (e.g., double materiality, value chain)
- **Enhance usability** and practical application (EU Taxonomy – simplified technical screening criteria)
- **Proportionality:** CSRD proposals reducing the scope to be more in line with CSDDD, delaying CSRD implementation deadlines for second and third wave of companies as per phased-in implementation and reducing reporting for smaller companies; CSDDD proposals postpone the first phase of application deadlines; EU Taxonomy application timelines will be impacted by above-mentioned delayed CSRD timelines
- **Simplification:** proposal to reduce mandatory datapoints for reporting, remove sector specific reporting requirements, and remove possibility of moving from limited to reasonable assurance
- **Enable digital reporting** through simplified templates.

Summary of the key proposed changes per regulation and timelines:

Area	Proposed Change	Target Implementation
CSRD	Streamlined disclosures; clarified double materiality assessments; reduced duplication with CS3D	2026 reports onwards
CS3D	Aligned due diligence scope with CSRD thresholds; simplified value chain due diligence	Post-2026
EU Taxonomy	Reduced granularity in technical screening criteria	From 2026

What you should be doing now – most imminent next steps:

At Capco, we believe that the EU Omnibus is a recalibration – one that reflects the EU's intention to make sustainability regulation scalable and effective. For our clients, it's a unique opportunity to:

- Review and realign ESG strategies with the new scoping and timelines and in light of the streamlined definitions (new scope and new timelines are particularly important for smaller companies).
    - Smaller firms: assess whether your timelines or obligations have changed, and plan accordingly
    - Larger firms: continue existing preparations (e.g., DMA) but adjust implementation plans to reflect expected simplifications (e.g., reduced disclosure granularity, clarified value chain scope).
- Optimize ESG data and reporting systems for digital ESG compliance by engaging with internal data owners and tech teams to scope what automation and system upgrades may be required.
- Anticipate, don't wait: While still in draft, the direction of travel is clear. Start aligning reporting and due diligence processes early for future efficiencies.

Looking ahead – what you should keep in mind

- Finalization is expected in late 2025, with staggered implementation from 2026 to 2028 – firms should monitor the legislative process and prepare for phased compliance.
- Expect additional technical guidance from EFRAG and the Commission, including on simplified templates and disclosures.
- Simplification doesn't mean ESG compliance rigor is going away – regulators are making requirements stickier and more usable. Firms that invest now will be better positioned to lead as the new framework settles.





How Capco can help

- **Regulatory advisory and assessing readiness**
  We partner with organizations to design and refine their sustainability strategy, targets and key performance indicators (KPIs), as well as disclosure roadmaps in alignment with the updated Omnibus Directive timeline. Our experts can help you navigate the applicability and scope of regulatory sustainability reporting based on the latest CSRD thresholds, ensuring your business remains resilient and strategically aligned with both regulatory expectations and internal business objectives.

- **End-to-end sustainability reporting and disclosure support**
  We provide comprehensive support across all aspects of sustainability disclosure and reporting, enabling our clients to act proactively in response to emerging frameworks such as CSRD, the CS3D, and other relevant regulations. Our services include conducting and automating Double Materiality Assessments – helping you to identify, embed, and respond to key risks, opportunities, and impacts. We ensure your reporting approach is not only compliant, but that it is also pragmatic and value-driven.

- **Strategic approach to ESG data and technology**
  We help clients to develop a more strategic approach to ESG data sourcing, data management and usage. We observe a common industry trend across our clients – to centralise the ESG data utility and to improve the way ESG data is used across functions. At Capco, we help clients to design their ESG data strategy, optimize data vendors, develop ESG data management platforms (either in house or leveraging external providers), and build business intelligence data tools to improve business decision making as well as reporting.

8. ESG scenario analysis and long-term strategy

Background

The European Banking Authority (EBA) published a draft of its guidelines for scenario analysis concerning ESG risks on January 16, 2025. Even if these guidelines are not final and the final publication date is not communicated, financial institutions need to work on the required implementation of these guidelines as they aim to support financial institutions in assessing their resilience against climate-related and other environmental risks while adapting their strategies for the long term.

They complement the 2024 EBA guidelines on integrating ESG risks into risk management and capital planning. For larger institutions subject to the Capital Requirements Regulation (CRR), these guidelines will take effect from 2026, while smaller and non-complex institutions (SNCIs) need to comply with them by the beginning of 2027. The draft guidelines define two primary objectives for scenario analysis:

1. **Financial resilience assessment** requires financial institutions to test their capital and liquidity provisions under various ESG scenarios.

2. **Long-term business model resilience** with a focus on evaluating the impacts of transitioning to a climate-neutral economy and the enduring effects of climate change.

Financial institutions are required to develop scenarios covering both physical risks (e.g., natural disasters) and transition risks (e.g., carbon pricing or regulatory changes). These scenarios aim to demonstrate how such risks could affect the financial stability and business strategy of financial institutions. Besides scenario development, financial institutions must identify mechanisms through which ESG risks could translate into financial risks, such as asset devaluation or increased credit risks in affected sectors. Integrating this scenario analysis into existing risk management processes is crucial for a continuous and systematic assessment of ESG risks. SNCIs will have more flexibility in data collection and methodology selection and may use qualitative assessments instead of quantitative analyses, ensuring that smaller financial institutions can comply without disproportionate burdens. Additionally, integrating

EBA Guidelines on ESG scenario analysis are to be issued pursuant to the EBA's mandate under Article 87a(5) of the Capital Requirements Directive VI (CRD VI) – application from January 2026 (January 2027 for small institutions)

EBA released its final Guidelines on ESG Risks including transition plan disclosure and implementation in CSRD and CSDDD – application from January 2026 (January 2027 for small institutions)

EBA Guidelines details how financial institutions should articulate their preparedness to respond and mitigate material ESG risks that could affect them

Embedding ESG Risk Management: The EBA's recent guidelines for ESG risk management and scenario analysis

These guidelines provide a structured approach to addressing ESG risks while highlighting their long-term impact on financial institutions.

scenario analysis into the Internal Capital Adequacy Assessment Process (ICAAP) is vital. Financial institutions must incorporate ESG risks into their capital planning and consider these risks over at least ten years. If scenario analysis indicates that ESG risks threaten capital provisions, financial institutions must adjust their capital strategies accordingly. This long-term perspective is essential because the effects of climate risks may only become apparent in the coming decades. Therefore, financial institutions must act in a timely manner to adjust their capital provisions and remain resilient.

What should firms do?

Developing and implementing the required ESG risk scenarios will present the biggest challenge for financial institutions, especially given the multitude of possible physical and transition risks that may impact their operations. Developing realistic scenarios and integrating them into existing risk management processes requires in-depth analyses and extensive data. Financial institutions must select appropriate models and assumptions to account for both the physical impacts of climate change (e.g., natural disasters or extreme weather events) and regulatory transition costs (e.g., carbon pricing or stricter environmental requirements). Forward-looking institutions should also use this requirement to automate both the newly required as well as existing analysis processes to reduce the additionally required efforts.

While in general the guidelines need to be applied as of 2026, smaller financial institutions are initially exempt from the guidelines. Nonetheless the development of their ESG strategies by 2027 requires making necessary structural adjustments that can be challenging for smaller institutions.

In either case, the creation of the additional scenarios' procedures requires investments in technology, expertise, and long-term employee training, which can be an additional burden.

The creation of the transition plans will further require detailed analysis to enable the definition of both pragmatic interim goals (e.g., focus on sustainable finance) for 2030 and strategic long-term goals for 2050 (e.g., net zero). A focus on prioritized levers and the setup of transparent monitoring are essential for an efficient integration of these goals in the operative processes and the strategic planning of the institution.

How Capco can help

Navigating the complexities of ESG risk scenarios and a comprehensive transition plan requires a strategic, holistic approach. We can support financial institutions with:

- **Regulatory expertise:** Providing deep insights into ESG risk and scenarios (especially also the newly required social and governance scenarios) and helping financial institutions identify and implement them effectively.
- **Technical implementation:** From identification and delivery of required data to adjustment of the affected processes and updating the calculation and reporting systems, Capco offers end-to-end technical support to ensure compliance.
- **Change management:** Capco assists in managing organizational changes, from training staff to redesigning business processes.

Navigating the complexities of ESG risk scenarios requires a strategic, holistic approach.

- **Innovation and strategy:** Capco identifies opportunities for innovation, driving efficiency through automated analysis processes and helps institutions stay competitive in the open finance era.

By effectively integrating and, when applicable, automating scenario analysis and adapting strategies to ESG risks, financial institutions can optimize their lending and investment portfolios, potentially benefitting from sustainable investments in the long term.

Capco is looking forward to supporting financial institutions along the way.



Developing and implementing the required ESG risk scenarios will present the biggest challenge for financial institutions - integrating them into existing risk management processes requires in-depth analyses and extensive data.

Christian Bergner
Principal Consultant

back to contents

9. Adoption of the International Sustainability Standards Board (ISSB) standards: A closer look

Since the International Sustainability Standards Board launched its first two sustainability-related standards (IFRS S1 and S2) in June 2023, the adoption or the full alignment of the standards is steadily gaining momentum. According to the IFRS foundation[3], 17 jurisdictions have adopted the ISSB standards and another 16 jurisdictions are in progress of adopting the standards as of June 2025.

Status[4]		Jurisdiction
Adopted	Fully adopting ISSB Standards	Mexico, Pakistan, Zambia
	Adopting ISSB Standards with limited transition	Malaysia, Tanzania
	Partially incorporating ISSB Standards	Australia, Bangladesh, Hong Kong, Sri Lanka, Turkey
	Permitting the use of ISSB Standards	Brazil, Chile, Ghana, Hong Kong, Jordan, Kenya, Nigeria
In progress of adopting		16 Jurisdictions (e.g., Canada, Singapore, South Korea, Thailand, United Kingdom)

What is ISSB?

ISSB aims to address the fragmented landscape of existing reporting frameworks by proving a single baseline for companies around the world to disclose their sustainability and climate-related risks and opportunities.

IFRS S1 General Requirements for Disclosure of Sustainability-related Financial Information offers a comprehensive framework for general sustainability-related disclosures, covering a range of environmental, social, and governance (ESG) topics.

IFRS S2 Climate-related Disclosures focuses specifically on the disclosure of climate-related financial risk and opportunities.

In April 2025, the ISSB published an exposure draft with proposed amendments to IFRS S2 standards. The exposure draft is open for comment until late June 2025, and the ISSB expects to finalise the amendments by the end of this year.

Five key challenges of ISSB-aligned disclosures

The process of alignment with the ISSB standards is not a simple "once-and-done" exercise. It takes time to gather the right quality of data and to adapt and extend existing processes.

Below we have summarized five common challenges we observed across our clients:

1. Cross-departmental engagement and collaboration

Achieving broad support from all relevant departments is crucial for successfully implementing new or additional ISSB climate disclosure requirements. This transformation requires changes to existing climate-related processes and policies

3. IFRS – Use of IFRS Sustainability Disclosure Standards by jurisdiction.
4. Please refer to 'Section 3.4 – Jurisdictional approaches to adopt or otherwise use ISSB Standards" of the IFRS Foundation's Inaugural Jurisdictional Guide for detailed definition of the ISSB adoption approaches.



across the organization. Departments may need to take on new responsibilities or create new roles. A cross-departmental approach is key, as sustainability and climate change management cannot be handled by one department alone.

2. Enhanced evaluation of the financial impact of climate-related risks and opportunities

Companies must perform scenario analyses to assess how physical and transitional risks and opportunities could affect their operations, investment and lending portfolios across various plausible scenarios and timeframes. It is crucial for financial institutions to define the key metrics that link material risks and opportunities to the financial statement line items most likely to be impacted.

3. Reliable accounting and target setting for Scope 3 emissions

Scope 3 emissions represent the broader value-chain emissions not directly controlled by the reporting entity. Reporting these emissions presents challenges, such as developing methodologies to assess the 15 categories from the Greenhouse Gas Protocol, evaluating sector-specific target-setting methods, sourcing quality data from suppliers and clients, and identifying reduction strategies aligned with targets.

Financial institutions must also measure and set targets for “financed emissions,” “facilitated emissions,” and “insurance-associated emissions” related to their investment, underwriting, lending portfolios, and capital market activities.

4. Enhanced IT infrastructure to absorb the burden on processes

Climate-related data requirements are more complex than others in the environmental and social spheres. To streamline data collection and assessment, it’s essential to digitalize and automate these processes. This approach facilitates the handling of large data volumes, enables continuous monitoring, and improves data quality. One effective solution is establishing a centralized ESG data utility.

5. The need for upskilling and capacity building

Financial institutions must develop internal capabilities to manage climate-related risks across the company. This often involves training workshops and regular working group meetings to ensure that all stakeholders understand the material climate-related risks and opportunities relevant to the company, the implications of its climate commitments and targets, and the essential components of the transition plan.

How Capco can help

Regardless of where you are on the climate disclosure journey, we can support you in navigating climate disclosure initiatives through our advisory in the following areas:

Greenhouse gas emissions accounting	Measure and understand your Scope 1-3 emissions using methodologies in accordance with the GHG Protocol and aligned to international assurance standards.
Climate risk assessment and integration	Conduct scenario-based climate risk and opportunity assessment to identify physical and transition risks material to your business and operations.
ISSB-aligned sustainability disclosures	Perform climate disclosures alignment reviews against peers and ISSB standards and assist in drafting the climate risk disclosures for reporting to align with the regulatory requirements.
ESG data solutions	Implement a centralized data solution that integrates seamlessly with the existing IT architecture to enable the transition from manual data collection processes to a more efficient and streamlined approach.
Capacity building	Design and implement workshops or learning programs to build internal awareness and capabilities for managing climate-related risks across the enterprise and facilitate cross-functional collaboration.

10. Navigating the new EU Sustainability Regulations

Summary

The European Union's (EU) latest wave of climate and environmental regulations, namely the Carbon Border Adjustment Mechanism (CBAM), the EU Deforestation Regulation (EUDR), and Phase 5 of the EU Emissions Trading Scheme (EU ETS), marks a significant shift toward enforceable sustainability compliance across global supply chains. These policies are not only reshaping how industries report and manage carbon emissions, but also introducing new demands for traceability, geolocation data, and real-time monitoring.

For global businesses, the implementation challenges are immense. From collecting granular emissions data from distant suppliers to integrating geospatial traceability tools, firms must now rapidly upgrade their data infrastructure and digital capabilities.



1. The EU Carbon Border Adjustment Mechanism (CBAM)

The Carbon Border Adjustment Mechanism (CBAM) is a carbon pricing policy introduced by the EU to reduce greenhouse gas emissions and create a fair, competitive environment between EU-produced goods and imports. It aims to address carbon leakage where companies might relocate production to countries with less stringent environmental regulations to avoid carbon pricing. By placing a price on embodied carbon from raw material extraction to manufacturing and transport, CBAM incentivizes cleaner production practices in non-EU countries.

The Carbon Border Adjustment Mechanism becomes fully effective on January 1, 2026.

CBAM applies to carbon-intensive goods, including electricity, hydrogen, iron, steel, and aluminum. Importers who fail to report emissions accurately, under-report emissions, or do not follow the required standards will face fines. The policy is currently in a transitional phase and will become fully effective on January 1, 2026.

Key technological challenges:

- **Data complexity:** Importers must gather emissions data from non-EU suppliers, many of whom lack standardized reporting infrastructures.
- **Verification:** Data integrity is difficult to ensure, particularly in jurisdictions with weak environmental governance.
- **Technology gaps:** There are few integrated tools to track and report emissions in real-time to the CBAM registry.

Strategic considerations to address the challenges:

- **Supplier data integration:** Deploy automated carbon data pipelines using IoT sensors and AI-based emissions calculators.
- **Blockchain verification frameworks:** Partner with audit firms to deliver secure, immutable emissions records.
- **Client training and advisory:** Support clients with reporting workflows and compliance navigation within EU portals.

2. EU Deforestation Regulation (EUDR)

The EU Deforestation Regulation (EUDR) is a landmark policy aimed at eliminating deforestation-linked goods from the EU market. It applies equally to EU and non-EU producers, covering key commodities such as palm oil, coffee, cocoa, timber, and soya. Under the regulation, deforestation is broadly defined as any conversion of forest to agricultural use, regardless of whether it is human-induced or caused by natural factors, and applies retrospectively to land cleared after December 31, 2020.

Companies within the scope must demonstrate that their products are deforestation-free through enhanced supply chain due diligence, comprising:

- **Information gathering:** Collect precise data on product origin, including geolocation of production plots and supplier details.
- **Risk assessment:** Evaluate environmental and human rights risks associated with the supply chain.
- **Risk mitigation:** Address identified risks through independent audits, field inspections, or supplier engagement.

A key part of the new rules is that firms must submit a formal due diligence statement to EU authorities, confirming compliance. EUDR enforcement begins on December 30, 2025 for large- and medium-sized operators and traders. Failure to meet the regulation could lead to substantial penalties, up to 4% of EU-wide turnover, reflecting the value and environmental impact of the offending products.

Capco has identified the following key technological challenges:

- **Traceability:** Mapping commodity origins to specific plots via geolocation data is labor-intensive and often opaque due to intermediaries.



- **Data fragmentation:** Supply chains lack standardized data-sharing practices.
- **Technology limitations:** Few tools integrate Global Positioning System (GPS), satellite imaging, and compliance documentation in one platform.

The following strategic considerations have been identified by Capco to address key technological challenges:

- **Geospatial intelligence platforms:** Build end-to-end platforms that combine satellite imagery, Geographic Information System (GIS) tools, and AI to map supply chains to plot-level precision.
- **Supplier portals:** Facilitate direct uploads of compliance documentation (e.g., GPS coordinates, land-use permits).
- **Deforestation risk dashboards:** Leverage machine learning to flag at-risk commodities and suppliers using global deforestation datasets.

3. EU ETS Phase 5

The European Union Emissions Trading System (EU ETS) is the EU's flagship climate policy and the world's largest carbon market. Its primary goal is to reduce emissions in a market-driven way, using the "cap-and-trade" principle. A cap is set on the total emissions allowed, and companies must hold allowances (EUAs) for every ton of CO_2 they emit. It promotes low-carbon investment by putting a price on carbon, and the EU ETS incentivizes companies to invest in cleaner technologies, energy efficiency, and renewable energy.

The EU ETS underpins the EU's climate targets, Phase 5 builds on earlier phases but introduces more ambitious climate targets aligned with the EU Green Deal, aiming to reduce emissions by at least 62% by 2030, compared to 2005 levels, and go towards the broader ambition of reaching climate neutrality by 2050. Phase 5 includes new sectors such as road transport fuels in 2027.

The implications for breaches are significant, ranging from substantial fines and financial penalties to reputational harm and potential legal action.

Capco has identified the following key technological challenges:

- **Real-time monitoring:** As free allowances shrink, companies must precisely measure and report emissions to avoid financial penalties.
- **Carbon price volatility:** Market dynamics demand agile trading and hedging strategies.
- **Legacy IT systems:** Many organizations still rely on outdated infrastructure that cannot meet the new regulatory demands.

The following strategic considerations have been identified by Capco to address key technological challenges:

- **Advanced emissions monitoring:** Implement real-time monitoring using IoT sensors at generating units and maritime fleets.
- **Carbon market analytics:** Develop algorithms that forecast EU carbon prices and support dynamic trading strategies.
- **IT infrastructure modernization:** Upgrade or integrate legacy systems to align with Phase 5 reporting requirements.

Data-driven initiatives to unlock strategic value

Meeting the demands of the EU's sustainability regulations requires a step-change in how companies collect, manage, and operationalize data across global operations and supply chains. The following data-driven initiatives are essential to enabling compliance and unlocking strategic value:

- **End-to-end environmental data infrastructure:** Build centralized data architecture that connects emissions, supply chain, and regulatory data into a single source of truth. This includes integrating disparate systems (e.g., ERPs, carbon accounting tools, supplier databases) to support consistent, accurate, and auditable reporting across CBAM, EUDR, and EU ETS.

- **Compliance automation and regulatory reporting:** Automate generation of due diligence statements, CBAM emissions declarations, and EU ETS reports by linking structured data directly to EU compliance portals. Use rules-based engines to validate entries before submission and reduce error rates.

- **Master data governance and traceability:** Establish robust data governance frameworks to ensure traceability, version control, and auditability of environmental data across business units and suppliers. Define clear ownership of emissions and sustainability data, backed by enterprise-grade metadata standards.

- **Geospatial data integration for EUDR:** Utilize geolocation data and satellite imagery to verify land-use history. This supports evidence-based assessments of whether commodities originated from deforested land. Embed GIS layers into supply chain management platforms to visualize and analyze risks. Standardize input formats to streamline reporting to EU authorities.

- **Supplier data digitialization and validation:** Develop supplier-facing data portals where producers and traders can upload required emissions, land-use, and product origin data. Enhance with automated data quality checks to flag incomplete or inconsistent entries. Incorporate third-party verification layers using blockchain or timestamped digital ledgers to ensure data integrity.

- **Advanced data analytics and risk modeling:** Apply machine learning and AI models to assess deforestation risks, detect anomalies in emissions reports, and forecast carbon pricing trends. These models help prioritize risk mitigation efforts and support trading strategies under EU ETS.

- **Real-time dashboards and alerts:** Create dynamic dashboards that visualize compliance status, data gaps, and upcoming regulatory milestones. Real-time alerts can flag when emissions exceed limits, data is missing, or due diligence obligations are at risk of being missed.

Conclusion

EU sustainability regulations are fundamentally data-driven mandates. Success depends not just on policy awareness but on building the data infrastructure, governance, and intelligence required to comply at scale. Companies that invest in robust, interoperable, and intelligent data systems will be better equipped to reduce risk, lower costs, and lead in a carbon-regulated global economy.

How Capco can help

Capco is ideally placed to help clients transition from reactive compliance to proactive sustainability leadership. By offering intelligent data architecture, cutting-edge technology, and strategic advisory, Capco enables organizations to navigate complexity, unlock efficiencies, and future-proof their operations in a climate-conscious world.



11. Addressing customer vulnerability – the challenge continues

Summary

The FCA's guidance for supporting vulnerable customers was introduced over four years ago, and yet the regulator's recent review shows that firms have still not yet fully engaged with the concept in a way that delivers consistently good outcomes for customers. As the UK's economic environment remains challenging, the incidence of vulnerability remains high, and characteristics of vulnerability impact how customers engage with both their financial services and energy providers. Firms in both sectors need to pivot their thinking on vulnerability to build consideration and support more extensively into their culture, processes, and risk monitoring. Management of data and use of emerging technologies are critical to identifying and supporting vulnerable customers.

Vulnerable customers continue to receive poor outcomes

In March 2025, the FCA set out the results of their Vulnerability Review and while they identified some areas of good practice – with renewed focus provided by the Consumer Duty – they also set out how vulnerable customers are continuing to receive poor outcomes. This is despite their guidance for supporting vulnerable customers[5] being in place since February 2021. In their review, they laid out key areas for improvement[6]:

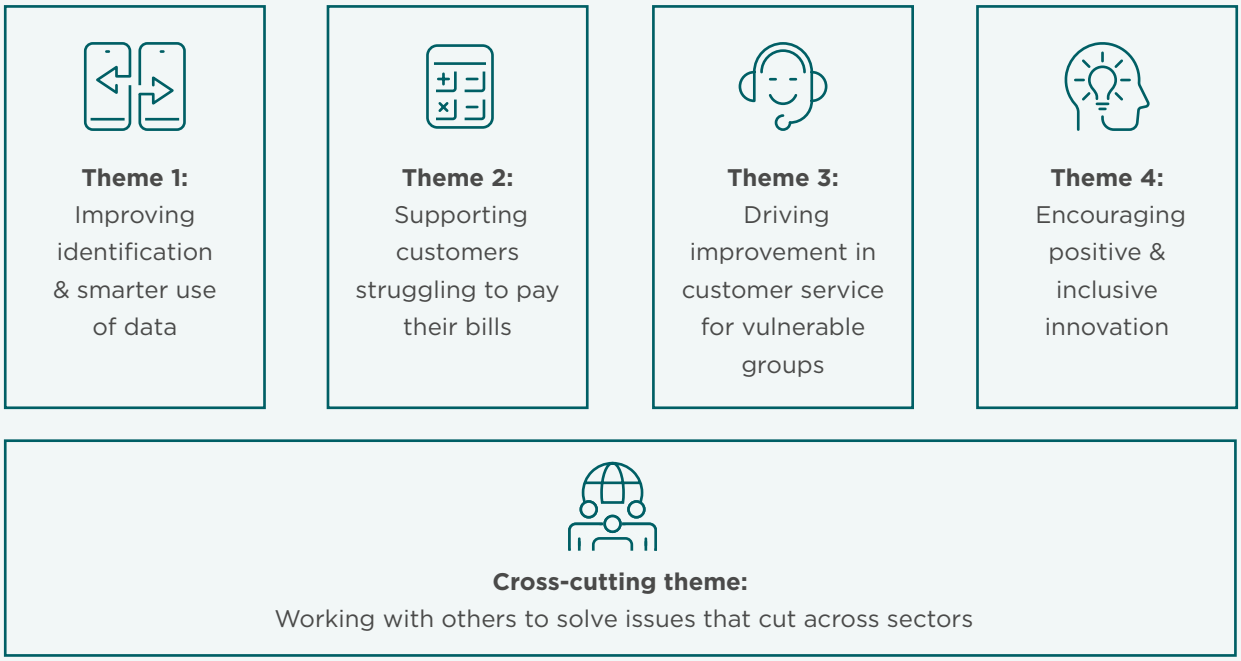
Areas for improvement	
Ineffective outcomes monitoring	Firms unable to show how they effectively monitor and take action on outcomes for customers in vulnerable circumstances. This included not being clear on what good outcomes look like or having clear ways of measuring them, not escalating issues, and lack of challenge or direction from senior leaders.
Failure to give appropriate support	Some firms failed to appropriately support staff in identifying customers in vulnerable circumstances, encourage customer disclosure, or provide support promptly and with an appropriate level of care.
Failure to communicate clearly to meet the needs of customers in vulnerable circumstances	Firms not providing appropriate or accessible channels to customers in vulnerable circumstances and a lack of testing of consumer understanding. Lack of consistency in providing clear information and communications not tailored to meet customer needs.
Lack of tailored training and embedding consumers' needs into product and service design	Most firms the FCA engaged with could not show how they had embedded the needs of customers in vulnerable circumstances into their product and service design processes. The FCA also saw a lack of training on vulnerability for product and design staff.

5. FG21/1 – Guidance for firms on the fair treatment of vulnerable customers, February 2021
6. Firms' treatment of customers in vulnerable circumstances – review, March 2025

Vulnerability is a key area of focus across financial services and energy sectors

More recently, Ofgem have also announced their Consumer Vulnerability Strategy[7], which is aligned with the FCA in focusing on identifying customers, providing appropriate treatments, and embedding consideration of vulnerability across the sector, to deliver better outcomes for customers.

Figure 1: Ofgem Consumer Vulnerability Strategy – strategy at a glance



While the language and strategic priorities differ slightly between Ofgem and the FCA, there is close alignment on the principle that firms must be efficient in identifying customers with characteristics of vulnerability and providing appropriate support for them.

The biggest challenges still outstanding

- Firms often struggle to accurately identify vulnerable customers, particularly those with non-visible vulnerabilities
- Defining what a good outcome is – there is no simple definition, but this requires clarity of articulation, otherwise firms don't know what they are aiming for
- Firms not having, or using, the right MI to give them a broad enough view of customer needs and behaviors
- Trust remains a barrier – vulnerable customers are still reluctant to disclose, for fear it will negatively impact their treatment
- Cultural blockers: there remains a perception that vulnerability is only an issue for front-line teams and doesn't need to be considered by others.

The risk of not addressing these challenges is customers suffering greater levels of harm, including digital exclusion, and making poor decisions that impact them financially.

7. Ofgem Consumer Vulnerability Strategy:



What firms should do

Firms across both sectors should focus on integrating vulnerability into their strategy and ways of working:

- Review their business strategy and integrate consideration of vulnerability as part of a customer-centric approach
- Proactively consider vulnerability as a key component in their data strategy
- Securely capture and manage key indicators of vulnerability (customer vulnerability data register) to build greater understanding of their customer base
- Deploy predictive models to proactively flag at-risk customers based on patterns in behavior or socioeconomic data
- Use GenAI to help identify vulnerability in real time, with targeted outreach
- Ensure that senior leaders embody a culture where all colleagues understand the part they play in delivering good outcomes for customers.

How Capco can help

Capco has experience of developing and implementing programs to support vulnerable customers across both financial services and energy sectors, and can support firms to:

Governance and outcomes monitoring	• Design and implement vulnerability strategy and frameworks • Design and build a customer vulnerability data register, incorporating real-time data feeds from multiple data sources
Consumer support	• Apply predictive models and GenAI to help identify characteristics of vulnerability in real time • Tailor digital propositions to provide effective consumer support
Consumer understanding	• Review and test customer communications
Products and services	• Build colleague capability in understanding and supporting customer needs

12. FS25/2: Transforming conduct risk management in the Consumer Duty era

Executive summary

In March 2025, the FCA published Feedback Statement 25/2 (FS25/2), outlining how it will simplify regulatory requirements in the wake of the Consumer Duty. The paper signals a shift from rule layering to simplification, requiring firms to take greater ownership of how they deliver good outcomes.

This is not deregulation – it is a recalibration. Oversight, judgement and accountability are now more important than ever.

A more focused approach to regulation

FS25/2 sets-out four themes: Reviewing The Foundations, Future-Proofing Disclosure, Reducing The Administrative Burden, and Streamlining Requirements. These actions are intended to support innovation and customer clarity while supporting high standards.

Figure 1: FCA's Planned Approach - from FS25/2

We are committed to an ambitious workplan:

Reviewing the Foundations	Addressing how we regulate and the scope of our rules, considering how they apply to customers based outside the UK and reviewing some core definitions.
Future-Proofing Disclosure	Allowing more flexibility to tailor customer-facing communications in a way which promotes consumer understanding and allows for more modern customer journeys.
Reducing the Administrative Burden	Giving firms more flexibility in how they apply our requirements, so that our regime is more outcomes-focused, reducing unnecessary administrative burdens.
Streamlining Requirements	Targeted work to remove or review outdated requirements, or areas of unnecessary complexity

The Consumer Duty provides the reference point for the shift in approach. Rather than relying on granular prescriptions, the FCA expects firms to use the Duty's principles to guide decisions – particularly when designing communications, products, and oversight frameworks. The simplification agenda is not about stepping back but about stepping differently, with more flexibility and more accountability.

For firms, this raises new expectations. Existing compliance models built around detailed guidance may no longer apply in the same way. Governance is not weaker but firms must have systems and controls that support sound, explainable decisions. The shift demands rigor, robust oversight, and outcome clarity.

Conduct delivery in a changing environment

FS25/2 introduces tangible shifts in how conduct regulation will be delivered across sectors, with the emphasis on flexibility, responsibility, and clarity of outcome:

- **Retail banking:** The FCA plans to revise prescriptive disclosure rules, including the summary box for savings accounts, to support clearer, more tailored customer communications in line with the Consumer Duty's focus on understanding and outcomes.

- **Insurance:** The regulator will consult on how the Duty applies to UK-based firms serving customers overseas. This includes whether the Duty should apply where international obligations already exist and how product governance expectations may vary for bespoke or international propositions.

- **Asset management:** The FCA intends to consult on changes to the public reporting requirement for annual value assessments, aiming to align these with broader reforms on assessing and evidencing fair value.

- **Regime-wide signals:** FS25/2 also commits to reviewing the Senior Managers & Certification Regime (SM&CR) and clarifying product governance and distribution expectations. Together, these initiatives suggest a future where firms hold greater discretion, and therefore greater accountability, in how they meet outcomes-based standards.

Stakeholder responses in FS25/2 make it clear: there is concern about the loss of certainty. Some firms worry that reducing prescription could create ambiguity and risk aversion. Others called for more guidance to help them manage oversight as rules evolve.

Ultimately, conduct maturity can become a differentiator. Firms should consider whether their existing control environments, including MI, escalation protocols, and product-level testing, remain robust enough in a more flexible regime. While the FCA does not prescribe how control environments should work, the need to deliver good outcomes under pressure is increasing.

Executive leadership insight: Interpreting responsibility, not waiting for permission

While FS25/2 does not explicitly direct boards or executive teams to change their structures or risk frameworks, it implicitly raises the bar for how leadership should think about oversight. The retirement of detailed guidance and withdrawal of legacy rules means firms must now show how their frameworks deliver good outcomes and not just follow instructions.

That does not require new controls everywhere, but it does require clarity. Leaders should consider whether their conduct risk governance and oversight arrangements can successfully function without granular regulatory direction. The same applies to assurance functions. As prescriptive rules recede, the burden of proof increasingly shifts to internal governance: can we explain what we did and how it served the customer?





Firms continue to face difficulty in articulating what a "good outcome" looks like, a challenge that grows in complexity as regulatory prescription recedes and judgement becomes central to evidencing compliance. Rather than suggesting new metrics or mechanisms, FS25/2 places emphasis on judgement, which is a leadership challenge as much as a compliance one.

Taking a more accountable approach

The simplification agenda laid out in FS25/2 potentially offers real benefits. Firms will be able to reduce duplication, simplify reporting and focus more directly on outcomes. But this flexibility comes with added accountability and firms will be expected to know – and show – that what they are doing delivers good outcomes and that senior management understands and manages key risks.

Firms that rely too heavily on being told what to do may find this uncomfortable. Those that see simplification as a mandate for maturity will be better placed to respond, lead, and differentiate themselves. The takeaway is that the standard has not dropped, rather the lens through which firms' compliance is measured has changed.

How Capco can help

Firms should be aware that the FCA will publish a substantive follow-up to FS25/2 in September 2025, which may further define expectations around simplification and conduct maturity.

Capco supports firms globally with complex regulatory transformation. We help clients to:

Immediate support

- **Strengthen conduct frameworks** by aligning them to evolving Duty expectations, especially in product, controls and oversight.
- **Enhance controls without reducing assurance:** supporting flexibility while preserving defensibility.
- **Improve customer understanding** and the ability to define and monitor customer outcomes where rule-based structures are being withdrawn.

Medium-term readiness

- **Support SM&CR readiness** by aligning leadership accountability to future simplification pathways.
- **Track regulatory simplification developments** and translate them into robust, auditable decisions.
- **Deploy Compliance Assist AI models to assess** regulatory coverage, flag gaps and enable auditable decision making.

Strategic capability building

- **Leverage behavioral and outcomes data** to enhance product relevance, journey design and Duty-aligned evidence.
- **Build judgement-led decisioning models** that enable confident conduct oversight.



“

The FCA’s plan to simplify regulation in the wake of Consumer Duty is not deregulation – it is a recalibration. Oversight, judgement and accountability are now more important than ever.

Jamain Graveney
Principal Consultant

▶ back to contents

13. Pure Protection Market Study

The Financial Conduct Authority (FCA) has recently launched its market study into pure protection insurance products, with initial findings and next steps due by the end of 2025. The study is designed to examine whether:

- the structure of commission encourages advisers to suggest when switching that may not be beneficial for consumers
- premiums are being raised by insurers to pay a higher commissions to an intermediary
- the products provide fair value
- the market supports innovation and growth,

The market study will focus primarily on the sale of four products: term assurance, critical illness cover, income protection insurance, and whole of life insurance. It will allow the FCA to carry out a more detailed analysis in these areas using its competition powers and the launch does not presuppose any particular outcome.

This comes off the back of work completed last year: in August 2024, the FCA published a final report pertaining to its **Thematic Review (TR 24/2)** of product oversight and governance for general insurance and pure protection. The review considered whether firms are meeting their product governance obligations for general insurance (GI) and pure protection under the new rules introduced by the regulator via the inclusion of fair value in the Product Governance sourcebook (PROD 4) in 2021 and the introduction in 2022/23 of the Consumer Duty.

The FCA expressed a sense of disappointment in seeing both manufacturers and distributors failing to meet their regulatory obligations under PROD fully, and considerations around further supervisory and regulatory actions are underway. Concern appears to be on distributors not fully understanding the distribution strategies in place or their responsibility to consider their remuneration, how this interacts with the services they provide, and its impact on the product's value.

To ensure the consistent provision of fair value to customers, firms should consider the entire foreseeable period, rather than focusing solely on the specific point in time when a product review is conducted. In addition, firms should utilize key data points that have been developed to continuously monitor whether customers are achieving the expected good outcomes. The value provided to customers through insurance products should be assessed using a variety of data points, such as claims rates or product usage (and cost), rejected claims rates (along with the reasons for rejections), customer journey drop-off rates, and customer sentiment analysis.

Initial findings from the FCA's market study and next steps are due by the end of 2025.

The nature of insurance products often leads to scenarios where third parties are used to either manufacture or distribute products. Therefore, it is essential that firms define the accountabilities and responsibilities throughout the entire product lifecycle and across the distribution chain. A key priority for insurers should be to ensure that key data points are being provided from third parties and that they are of sufficient quality to enable decision making. Equally, it is just as important for firms to be open to sharing information that is required by third parties to enable assessments of good customer outcomes. The governance and oversight of these metrics and the ongoing monitoring should be embedded into business-as-usual processes and forums, as part of conduct risk oversight: this will enable the identification of any potential areas of concern and drive any required actions to deliver good outcomes in line with the requirements of the Consumer Duty.

Firms falling within the scope of the Thematic Review have received direct feedback from the FCA. For other firms bound by PROD 4 and the



Consumer Duty, they can take a number of steps now to enhance their deliver of fair value and good outcomes for customers and prevent more direct regulatory intervention.

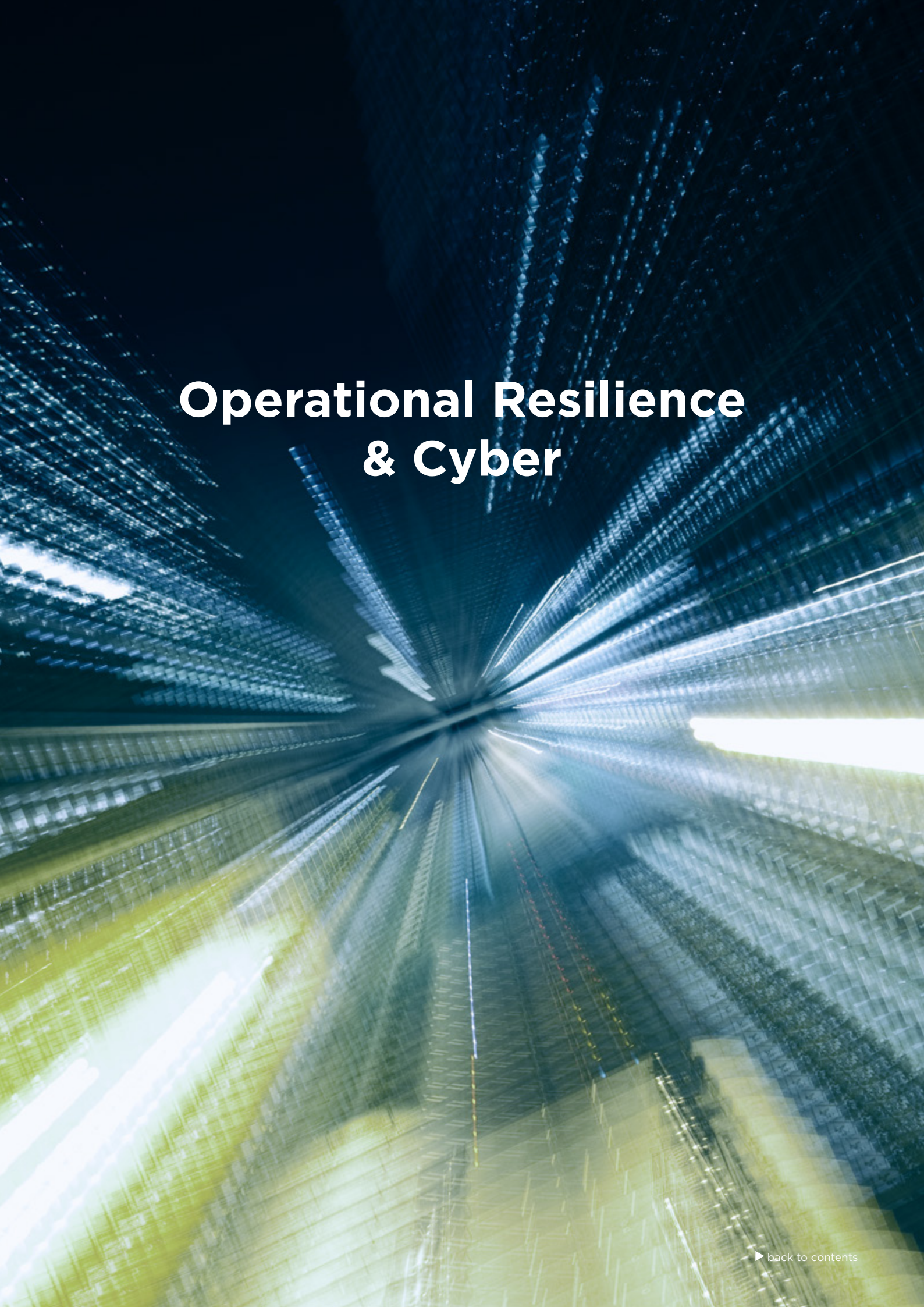
While awaiting the outputs from the study, we recommend focusing on four priorities

1. **Embed key concepts of Consumer Duty within your culture.** It is critical that the concepts of customer harm and good outcomes are central to firms' purpose and strategy, and that firms' actions are driven by customer focus, rather than purely commercial interests.

2. **Review commission arrangements**, both in terms of the proportionality and fairness of any payment to the premium paid by customers in relation to the product or service provided. Also consider how those commissions are disclosed, given the heightened focus on this with discretionary commission payments in the car finance industry.

3. **Carry out a holistic review of your product governance framework:**
   - Is there a consistent application of the framework across all business units?
   - Do your fair value assessments contain all the necessary considerations, such as total price across the value chain or the impact of remuneration paid to distributors?
   - Is your committee structure fit for purpose and can you demonstrate its operational effectiveness?
   - Is policy designed appropriately and applied consistently? Are relevant controls in place to enable effective risk management and product oversight?
   - Can you demonstrate how / where you are acting on appropriate insight to make effective decisions to mitigate or prevent harm?
   - Do you have clarity on where ultimate responsibility sits for product oversight and whether products provide fair value?

4. **Enhance the quality of your management information (MI)**. Effective decision making is almost impossible unless MI is appropriate, timely, sufficient and consistent where needed across products. The range of data should be broad, including customer surveys, complaints, call monitoring, file reviews, transactional analysis, and claims, with defined standards, tolerance, and rationale as to why they represent fair value. The regulator's own focus on data-driven decisions means that scrutiny on MI will continue, and the quality of firms' MI is the crucial component in delivery of good outcomes.



Operational Resilience & Cyber

back to contents

14. Navigating the evolving landscape of AI regulation in regulated industries



Summary

- The OECD AI principles[8] of transparency, accountability, fairness, robustness, and inclusive growth continue to guide legislators and regulators.
- Legislation, such as the EU's AI Act[9] and South Korea's AI Framework Act[10], reflect growing international consensus around risk-based AI governance[11,12].
- Regulators (for example, UK FCA, Bank of England[13], US Treasury, UK Ofgem[14], US DOE[15]) are increasingly focused on the systemic risks, consumer protection, and ethical implications posed by AI.
- AI alignment[16] and transparency remain critical challenges, impacting consumer trust, market stability, and regulatory compliance.
- Financial institutions must proactively embed OECD-aligned governance and robust risk management practices.

The rapid evolution and adoption of artificial intelligence has the potential to profoundly reshape the landscape for regulated industries including financial services and energy, driving both innovation and corresponding legislation and regulatory scrutiny. The OECD AI Principles of inclusive growth, human-centric values, transparency, robustness, and accountability provide the intellectual foundations for convergence, underpinning legislation, regulatory guidance, and policy responses globally.

The EU's AI Act is set to become one of the most stringent and comprehensive regulatory frameworks, explicitly reflecting OECD principles through a clearly delineated, risk-based approach. The AI act initially came into force in August 2024 with further phases planned through to 2030.

The AI Act classifies AI applications into use case risk-based categories, imposing heavy compliance obligations on high-risk use cases. Use case areas that can be considered high-risk include personal credit

8. https://oecd.ai/en/ai-principles
9. https://artificialintelligenceact.eu/
10. https://fpf.org/blog/south-koreas-new-ai-framework-act-a-balancing-act-between-innovation-and-regulation
11. https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/truly-riskbased-regulation-of-artificial-intelligence-how-to-implement-the-eus-ai-act/E526C1D0D7368F9691082220609D60F4
12. There are differences in approaches to how risk-based governance is applied, with the UK taking a less prescriptive, more flexible stance. Also see: https://www.nist.gov/itl/ai-risk-management-framework
13. https://www.bankofengland.co.uk/financial-stability-in-focus/2025/april-2025
14. https://www.ofgem.gov.uk/sites/default/files/2024-04/Ofgem%27s%20strategic%20approach%20to%20AI%20FINAL%20240430.pdf and https://www.ofgem.gov.uk/consultation/artificial-intelligence-ai-energy-sector-guidance-consultation
15. https://www.energy.gov/ai/artificial-intelligence-and-technology-office
16. AI alignment seeks to ensure that artificial intelligence systems reliably understand, follow, and act in accordance with human values, intentions, and ethical guidelines. By extension, alignment includes consistency with regulatory expectations and organizational risk appetites that embody these values and intentions.

scoring and risk assessment for insurance, as well as critical infrastructure[17]. While the AI Act explicitly recognizes the role of innovation, its focus is on responsible innovation. Transparency, explainability, and robustness are mandated by the act to safeguard consumer rights and ensure financial stability, aiming to maintain consumer trust and prevent systemic disruptions arising from algorithmic errors or biases.

South Korea's recently introduced AI Framework Act similarly aligns with OECD principles but adopts a notably different implementation strategy. In contrast to the EU AI Act, the South Korea Act focuses predominantly on promoting AI innovation first, then applying targeted regulatory safeguards for high-impact applications in sectors including financial services, like the UK's evolving approach. These contrasting approaches reflect a nuanced balance between fostering technological advancement and ensuring accountability, security, and ethical standards, demonstrating an ongoing debate between robust governance and technological progress.

Within financial services specifically, regulators have consistently highlighted challenges around AI alignment[18] and transparency. A recent Bank of England Financial Policy Committee (FPC) publication[19] underscores how AI-driven trading systems could exacerbate systemic risk by fostering herd behaviors and increasing market volatility, and advocates for clearer regulatory oversight. Key concerns raised include cybersecurity, model homogeneity from supplier concentration, as well as related operational dependencies.

The FCA's establishment of an AI Lab[20], aligned with the FPC's stress on continuous monitoring and engagement, highlights its commitment to addressing these challenges directly, with an initial "AI Sprint" at the start of 2025, to be followed by an AI testing service later in 2025[21]. The AI lab seeks to enable a practical way to engage with the industry to enhance AI transparency and accountability, and to better understand how AI can impact market conduct by enabling firms to check their AI tools meet regulation before being deployed. This is particularly important for consumer protection in areas such as credit assessment and automated investment decisions, consistent with the use case risk approach in the EU AI Act.

It is recognized that the inherent complexities of AI alignment and transparency can pose substantial risks to financial services[22]. Lack of transparency, particularly regarding automated decision-making processes, can exacerbate these risks, potentially leading to regulatory non-compliance, reputational damage, and even legal liabilities. Even so, regulators generally seek to support the potential value-add of using AI responsibly and with full transparency. The FCA's recent research[23], for example, emphasizes the importance of explaining AI-driven credit decisions clearly to consumers, reinforcing regulatory expectations around clear governance frameworks and human oversight.

The U.S. approach to AI regulation is characterized by a decentralized, sector-specific framework, emphasizing voluntary guidelines, industry-led standards, and minimal federal oversight to encourage innovation and competitiveness. Regulation primarily involves existing agencies addressing AI issues within their respective domains. The US approach was initially supported by the White House's AI Bill of Rights[24], which outlined broad ethical principles rather than binding regulations. The "Removing Barriers to American Leadership in

17. https://artificialintelligenceact.eu/annex/3/
18. https://alignmentsurvey.com
19. Financial Stability in Focus: Artificial intelligence in the financial system – https://www.bankofengland.co.uk/financial-stability-in-focus/2025/april-2025
20. https://www.fca.org.uk/firms/innovation/ai-lab
21. https://www.fca.org.uk/news/press-releases/fca-set-launch-live-ai-testing-service
22. https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024
23. FCA research note on the use of AI in credit decisions – https://www.fca.org.uk/publications/research-notes/credit-where-credit-due-how-can-we-explain-ai-role-credit-decisions-consumers
24. https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/

Artificial Intelligence"[25] order shifts focus towards reducing federal oversight and promoting innovation in AI.

Cybersecurity is also strongly emphasized by regulators globally. The UK's recent shift in focus from AI safety to AI security[26] reflects escalating concerns regarding AI-enabled cyber threats, further underscoring the importance of comprehensive cybersecurity frameworks within regulated industries. Regulators increasingly require institutions to integrate AI security into their broader cybersecurity risk management strategies.

Because the OECD principles provide a general framework that informs approaches to regulation across multiple industries and geographies, those principles help institutions operating at a global level. Adopting OECD aligned transparent and accountable approaches helps ensure clarity in AI operations and outcomes, reflecting consumer protection, fairness, and ethical values explicitly.

Equally critical is robust risk management capable of identifying, assessing, and mitigating systemic and individual risks related to AI deployment. Achieving true AI alignment requires ongoing efforts, proactive regulatory engagement, and continuous innovation to ensure AI tools remain ethical, robust, and beneficial to society and financial markets alike.

For regulated industries, key considerations are:

- **Increased compliance complexity:** evolving, nuanced AI regulations, requiring proactive alignment and potentially increased compliance costs
- **Balancing innovation and risk:** strategically navigate regulatory sandboxes and risk-based frameworks to innovate without compromising regulatory standards or consumer safety
- **Enhanced transparency and accountability:** robust governance structures, transparent AI systems, and clearer accountability to mitigate regulatory, operational, and reputational risks.

How Capco can help

We believe that integration and alignment of AI governance with existing risk governance operations during 2025 will position institutions to safely adopt and create value from AI investments through 2025/6, in alignment with the evolving regulatory landscape.

Capco offers comprehensive support to financial services and energy organizations navigating the complexities of AI regulation and governance, including:

- Deep regulatory expertise
- Strategic insights
- Practical experience in digital transformation and technology risk management
- AI-enabled regulatory compliance tools.

Capco helps our customers to implement effective data and AI frameworks with tailored advisory services, covering:

- AI transparency
- Explainability
- Risk management
- Cybersecurity
- Alignment challenges.

Partnering with Capco ensures your AI strategy meets regulatory expectations while fostering innovation, consumer trust, and competitive advantage in the evolving financial services landscape.

25. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/
26. https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice



> **The EU's AI Act is set to become one of the most stringent and comprehensive regulatory frameworks, explicitly reflecting OECD principles through a clearly delineated, risk-based approach.**
>
> **Charlotte Byrne**
> Managing Principal

▶ back to contents

Aspect	OECD	EU	South Korea	US
Type of approach	Principles-based	Risk-based, comprehensive regulatory	National strategic framework, sector-specific	Decentralized, voluntary standards, sector-specific
Key documents or policies	OECD AI Principles (2019)	EU AI Act (proposed 2021, finalized 2024-25)	National AI Strategy, AI Ethics Guidelines (2020)	AI Bill of Rights (2022, now de-emphasized), Executive Orders
Legal status	Non-binding recommendations	Binding regulation (mandatory compliance)	Mixed (guidelines, some binding laws)	Primarily voluntary guidelines, limited binding regulation
Primary objectives	Trustworthy AI, transparency, fairness, accountability	Protect fundamental rights, health, safety; manage risk	Innovation, ethical use, competitiveness, safety	Innovation, competitiveness, minimal regulatory burden
Risk management	General guidance on ethical AI use	Strict compliance requirements for high-risk AI	Ethical guidance and best practices, sector-specific regulations	Industry-driven, market-based approach with minimal federal intervention
Implementation method	International cooperation, member countries encouraged to adopt guidelines	Centralized regulatory oversight (EU-level enforcement)	Government-driven strategic initiatives with industry collaboration	Fragmented, sector-specific implementation via existing agencies and industry-led self-regulation
Enforcement and oversight	Voluntary adherence, limited enforcement mechanisms	Strong enforcement through EU Commission and national authorities	Moderate enforcement, primarily driven by government guidance and industry cooperation	Minimal centralized enforcement, reliant on existing regulatory agencies and voluntary compliance
Human rights and ethics emphasis	Strong emphasis on human rights, fairness, and transparency	Very strong emphasis on fundamental rights, transparency, and accountability	Significant emphasis on ethics, human-centric AI, transparency	Moderate to low emphasis, previously emphasized but reduced under recent administration
Data privacy and protection	Recommended best practices, aligns closely with existing data protection laws	Robust, strongly tied to GDPR and data governance regulations	Strong focus integrated with existing privacy and data protection laws	Moderate; sector-specific approach, no comprehensive national AI data privacy law
Biometric and surveillance regulation	General ethical guidelines against misuse, but non-binding	Strictly regulated, particularly for biometric and mass surveillance applications	Moderately regulated, specific restrictions in some areas (e.g., facial recognition guidelines)	Sector-specific restrictions, generally permissive with limited federal regulation

15. Regulatory focus post implementation of the UK Operational Resilience policy and Digital Operational Resilience Act



Key Headlines

- Regulatory attention moved from implementation to embedding of operational resilience.
- Ongoing assessment and testing to ensure firms can manage disruptions, with focus on identified cyber hygiene issues.
- Critical third-party providers will be designated and subject to regulatory oversight.
- UK regulators begin consultation around ICT and cyber resilience risk expectations in 2025 H2.
- FCA operational incident and third-party reporting policy expected later in 2025.

March 31, 2025 marked the end of the transition period for the UK Operational Resilience policy and the EU Digital Operational Resilience Act (DORA) has been in force since January 17, 2025. These regulations share the objective of improving the resilience of the financial sector against operational disruptions, requiring firms to identify and set impact tolerances for important business services / critical or important functions, perform resilience testing, and manage third-party risk.

Regulators have moved into "business-as-usual" mode, meaning firms can expect increased scrutiny through supervisory reviews, data requests, and targeted assessments.

Cyber

The ability for firms to detect, respond to, and, in particular, recover from cyberattacks is seen as a critical element in the resilience of the financial system.

UK regulators will continue to assess firms' capabilities to manage cyber threats with the ongoing use of threat-led penetration testing (TLPT) and cyber questionnaires. There will be a focus on the cyber-hygiene issues highlighted in the 2024 CBEST thematic findings, including identity and access management, configuration and vulnerability management. Firms should also consider the findings from the latest Cyber Stress Test being published later in 2025.

Similarly, DORA requires that financial entities must conduct TLPT at least every three years, covering several or all critical or important functions, and which must be performed on live production systems.

UK regulators will start consultation in 2025 H2 on the management of information and communications technologies (ICT) and cyber risks, including the ability for the sector to detect, withstand and recover from cyber incidents and risks arising from complex technology transformations.

Finally, as concerns around AI-enabled cyber threats grow, regulators increasingly require AI security to be integrated into existing cybersecurity frameworks.

Third parties

The UK regulatory authorities have set final policy supporting HM Treasury's designation of third-party service providers as "critical third parties" (CTPs) if their failure or disruption threatens UK financial stability.

Regulators have moved into "business-as-usual" mode, meaning firms can expect increased scrutiny through supervisory reviews, data requests, and targeted assessments.

Under DORA, the European Supervisory Authorities (ESAs) will use the ICT third-party arrangements reporting received from financial entities to assess critical third-party providers (CTPPs) by July 2025. The ESAs will notify and designate CTPPs and start oversight engagement with them. Third-party service providers not included may request designation once the CTPP list is published.

Following consultation, the UK policy on operational incident and third-party reporting is expected to be finalized in 2025, providing guidance on the definition of operational incidents, thresholds, reporting format and timelines, aligning with international standards. It also seeks to expand the scope of third-party reporting, notifications and registration arrangements, aligning with DORA and EBA outsourcing guidelines, reducing the regulatory burden on firms and enabling consistent data analysis.

Operational resilience embedding

With operational resilience policies now fully in force, regulatory authorities are expecting firms to be embedding operational resilience into enterprise-wide risk frameworks and culture. Therefore, operational resilience should be a key consideration in strategic planning and when assessing risks associated with change and transformation.

The UK regulatory authorities are working to strengthen domestic and international coordination across operational resilience, cyber, and third parties due to the cross-sector and cross-jurisdictional nature of services and infrastructure, including simulation exercises in collaboration with industry, to rehearse resilience capabilities and prepare for system-wide disruptions.

What should firms do?

Firms should continue the journey to embed and foster a culture of operational resilience, building sustainable and cost-effective strategic capabilities and demonstrate to stakeholders the commitment to managing service resilience posture.

- Utilize a global approach and framework to ensure consistency, alignment, and efficiency
- Continue to assess and enhance cyber resilience abilities, consider findings from CBEST and forthcoming Cyber Stress Test thematic reviews
- Strengthen cyber incident response and recovery
- Further develop third-party resilience by identifying and managing supply chain risks from fourth parties and beyond
- Validate new and existing capabilities through scenario tests of maturing scope and complexity.





How Capco can help

Achieving compliance and embedding operational resilience through alignment, integration and automation of capabilities can be challenging. Drawing on our deep sector, risk, regulatory, and technology expertise, we can support firms in the following areas:

- Assessing the maturity of cybersecurity posture and controls to prepare for and respond to audits and regulatory exams
- Executing cyber resilience programs to deliver enhancements and remediate identified gaps
- Implementing optimized governance, operating models, processes, controls, data, and technology
- Identifying, monitoring, managing, and reporting on third-party and supply-chain risks. Supporting firms to develop a strategic solution for the register of third-party arrangements
- Developing incident response and recovery frameworks, solutions, and playbooks
- Planning and executing scenario testing exercises, leveraging GenAI for dynamic scenario generation, interactive engagement, and enhanced immersion.

16. Australia's Prudential Standard CPS 230 – Operational Risk Management



Key Headlines

- The Australian Prudential Regulation Authority (APRA) has introduced **Prudential Standard CPS 230 – Operational Risk Management**, effective **July 1, 2025**.
- CPS 230 sets new standards for operational risk management and business continuity planning, including service provider arrangements in Australia's financial sector.
- Entities must identify critical operations, set tolerance levels, and report material incidents to APRA within 72 hours.
- CPS 230 applies to **all APRA-regulated entities** including banks, insurers, and superannuation trustees.

Core requirements of CPS 230

The regulation has laid down guidelines for developing the risk management framework, managing operational risk, ensuring continuity of critical operations, and managing risks arising from service providers. This is consistent with global trends in operational resiliency, such as the US OCC's emphasis on incident escalation and Europe's DORA. We believe CPS 230 will not only serve as a supervisory tool but also as a strategic transformation blueprint for ops resilience.

Risk management framework

APRA mandates that institutions integrate operational risk management into their comprehensive board-approved risk framework, which includes governance, risk appetite, controls, monitoring, incident response, BCPs, and management of service providers.

These elements should be routinely assessed according to CPS 220/SPS 220, in accordance with recovery and exit strategies, and may be subject to APRA action if significant deficiencies are found.

Operational risk management

Key risks under operational risk include legal and regulatory risk, compliance and conduct risk, technology and data risk, and change management risk.

Senior management is responsible for embedding the framework. The framework needs to be reviewed regularly and **independently assessed** at least **once every three years** [refer CPS 220 and SPS 220].

Operational risk profile and assessment

- Build **information systems** to monitor operational risk, analyse data, and report to senior management and the board
- **Document critical processes**, resources, interdependencies, and related risks, obligations, and controls.

Operational risk controls

Institutions must **implement** and **test controls** to manage operational risk, with timely remediation and clear accountability for any weaknesses.



> **We believe CPS 230 will not only serve as a supervisory tool but also as a strategic transformation blueprint for ops resilience.**

Shivaji Chakraborty
Partner

▶ back to contents

Incident management and reporting to APRA

Entities must have processes to identify, escalate, record, and resolve operational incidents and near misses. Material incidents must be reported to APRA as soon as possible, and no later than 72 hours after discovery.

Critical operations and tolerance levels

Entities have to register critical operations that can impact customers, markets, or institutional viability. Examples include payments and settlements (for ADIs), claims processing (for insurers), and investment management (for RSE licensees). For each operation, they have to set and document tolerances for downtime, data loss, and service levels. Tolerances must be reviewed at least annually.

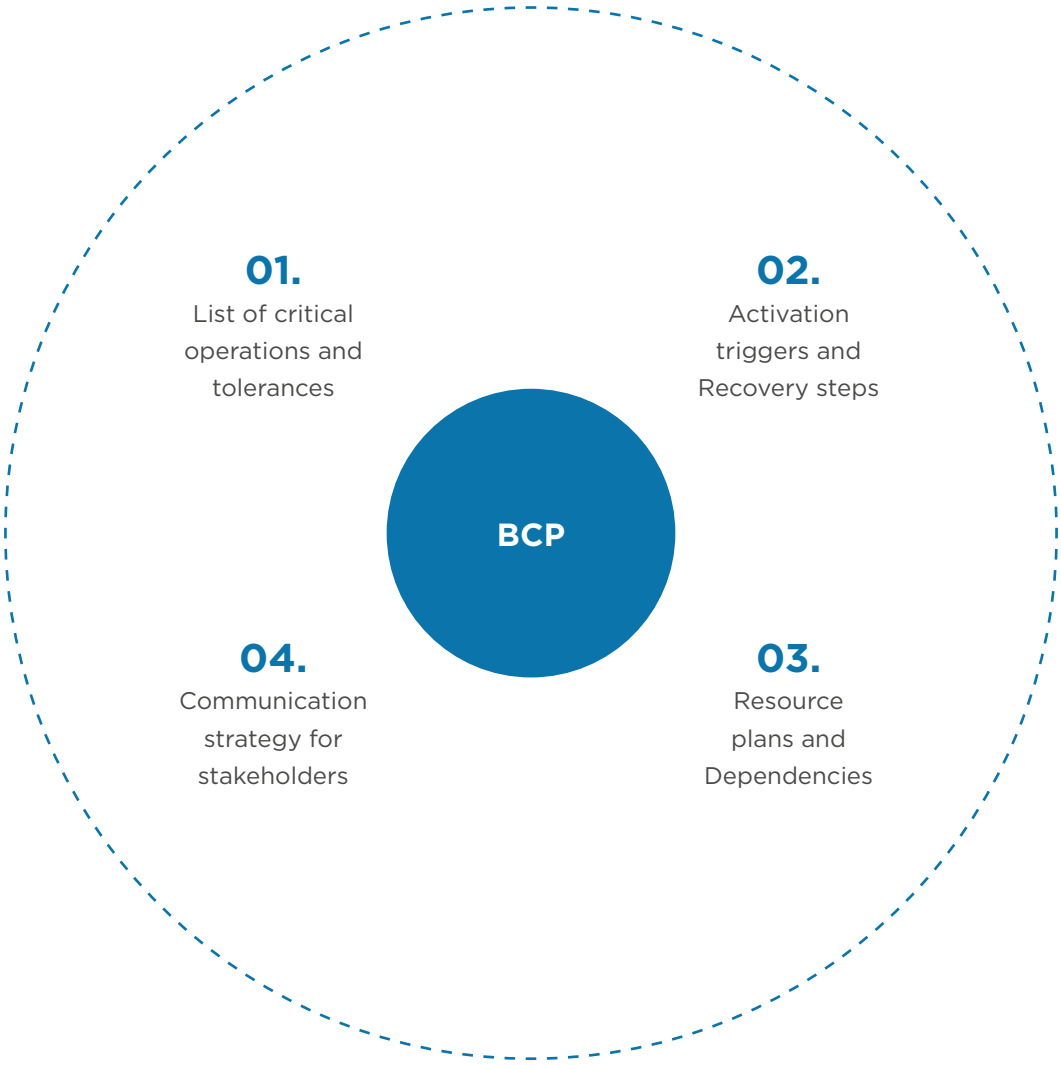
Business continuity planning

Institutions will have to maintain a business continuity plan (BCP) to ensure critical operations continue during disruptions and recover within defined tolerance levels.

Institutions will need to ensure they have the capability to execute the plan and must report any tolerance breaches and remediation actions to the board.

APRA should be notified as soon as feasible, **but no later than 24 hours**, if there is an interruption to a key operation **above the agreed tolerance**. The report should cover event, response, impact, and recovery timeline.

BCP components



Management of service providers

In order to manage service providers, entities need to create a policy. Finding material service providers is part of this.

Agreements need to contain clear-stated performance expectations as well as rights of access and audit. There are clauses pertaining to termination and transition.

Every year, APRA must receive a registration of material service providers. When entering into or significantly altering any such arrangement, APRA must also be informed **within 20 business days**.

Implications for financial institutions

The introduction of CPS 230 represents a **paradigm shift**. Institutions will need to:

- Embed **operational resilience** into strategic planning and enterprise risk management
- Conduct **gap assessments** against CPS 230 requirements and develop structured implementation roadmaps
- Strengthen **governance and board engagement** on operational risk oversight
- Build robust **incident response and crisis management capabilities**.



Those who delay may find compliance costly and rushed, risking reputational and supervisory penalties.

Firms can face multiple challenges around disjointed ownership of resilience in technology and business, manual tolerance mapping as well as compartmentalized risk registers and legacy contracts without APRA-mandated provisions. These need to be tackled immediately. Firms should think of designating a resilience lead under the chief risk officer. Implementation of integrated resilience tools for operations, cyber, and vendor risk convergence should be a priority. Contract renegotiation pipelines should be prioritized by triaging, using contract analytics. Usage of Python as well as AI/ML analytics will turn out to be a necessity for doing gap analysis of contracts against CPS 230 requirements.

Timeline and compliance expectations

Milestone	Requirement
CPS 230 Effective Date	1-Jul-25
Pre-existing service provider compliance	By 1 July 2026 or at contract renewal
APRA notification (material incident)	Within 72 hours
APRA notification (breach of tolerance)	Within 24 hours
BCP and tolerance review	At least annually
Framework independent review	At least every 3 years

How Capco can help

Capco's blend of risk, regulatory, cyber, and technology expertise positions us as the ideal partner to support you in achieving CPS 230 compliance, not just as a regulatory obligation, but as a strategic resilience advantage.

Our expertise covers:

- Gap assessments and readiness reviews against CPS 230
- Operational risk and resilience framework design tailored to regulatory expectations
- Critical operations mapping and resilience testing
- Third-party risk management and service continuity planning
- Board and senior management advisory on governance enhancements
- Incident response playbooks and crisis simulation exercises.



Sources

https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf

17. Cyber resilience in APAC: India & Hong Kong step up supervisory expectations



Key Headlines

- IFSCA India mandates a unified cybersecurity and cyber resilience framework for regulated entities, effective March 2025.
- The Hong Kong SFC's thematic review flags weaknesses in software patches, third-party access, and ransomware readiness for licensed internet brokers.
- Regulators expect financial institutions to institutionalize cybersecurity governance, response plans, and board-level accountability.

Cybersecurity comes into focus in APAC's financial hubs

Two recent announcements from major APAC jurisdictions emphasize how important it is to have strong, all-encompassing cybersecurity programs in order to keep pace with the financial markets' explosive growth in digital use.

- In March 2025, India's International Financial Services Centres Authority (IFSCA) issued their comprehensive Guidelines on Cyber Security and Cyber Resilience, aimed at all regulated entities.
- In January 2025, Hong Kong's Securities and Futures Commission (SFC) shared results from their Report on the 2023/24 thematic cybersecurity review of licensed corporations.

These changes point to a changing supervisory strategy that goes beyond simple detection and response to include prevention, governance, and recovery.

India IFSCA Guidelines: A comprehensive cybersecurity blueprint

The IFSCA guidelines apply to all organizations governed under its scope (banking, insurance, capital markets, etc.) and outline a thorough, principle-focused approach to cybersecurity. Here are the main points:

Governance: Regulated entities must establish clear roles and responsibilities for managing cyber risks, led by an oversight body having a designated officer, such as a CISO.

Cybersecurity and cyber resilience framework: This framework focuses on maintaining the confidentiality, integrity, and availability (CIA) of IT assets. An information security (IS) policy will have to be formulated consisting of identification and classification of IT assets, appropriate security controls, access control of IT assets, physical security of IT assets, data centers and server rooms, vulnerability assessment and penetration testing (VPAT), recovery policies, cyber-incident management and audit trails.

Third party risk management: Regulated entities are responsible for ensuring that third-party vendors adhere to the same cybersecurity standards.

Communication and awareness: Regular cybersecurity training for employees is mandatory.

Audit: Annual independent audits are required to assess the effectiveness of the cybersecurity framework, with reports submitted to IFSCA within 90 days of the financial year-end.

Incident reporting: Cyber incidents must be reported to IFSCA within six hours of detection, followed by an interim report within three days and a detailed analysis within 30 days.

The circular is effective from **April 1, 2025.**

Hong Kong SFC: Report on the 2023/24 thematic cybersecurity review insights

The Securities and Futures Commission (SFC) released its 2023/24 report on the cybersecurity thematic review, focusing on licensed internet brokers' adherence to cybersecurity requirements. Between 2021-2024, eight material events were reported, including ransomware attacks and compromised vendor systems, mainly due to outdated software and inadequate internal controls.

1. Key deficiencies identified

The review found multiple lapses in cybersecurity controls:

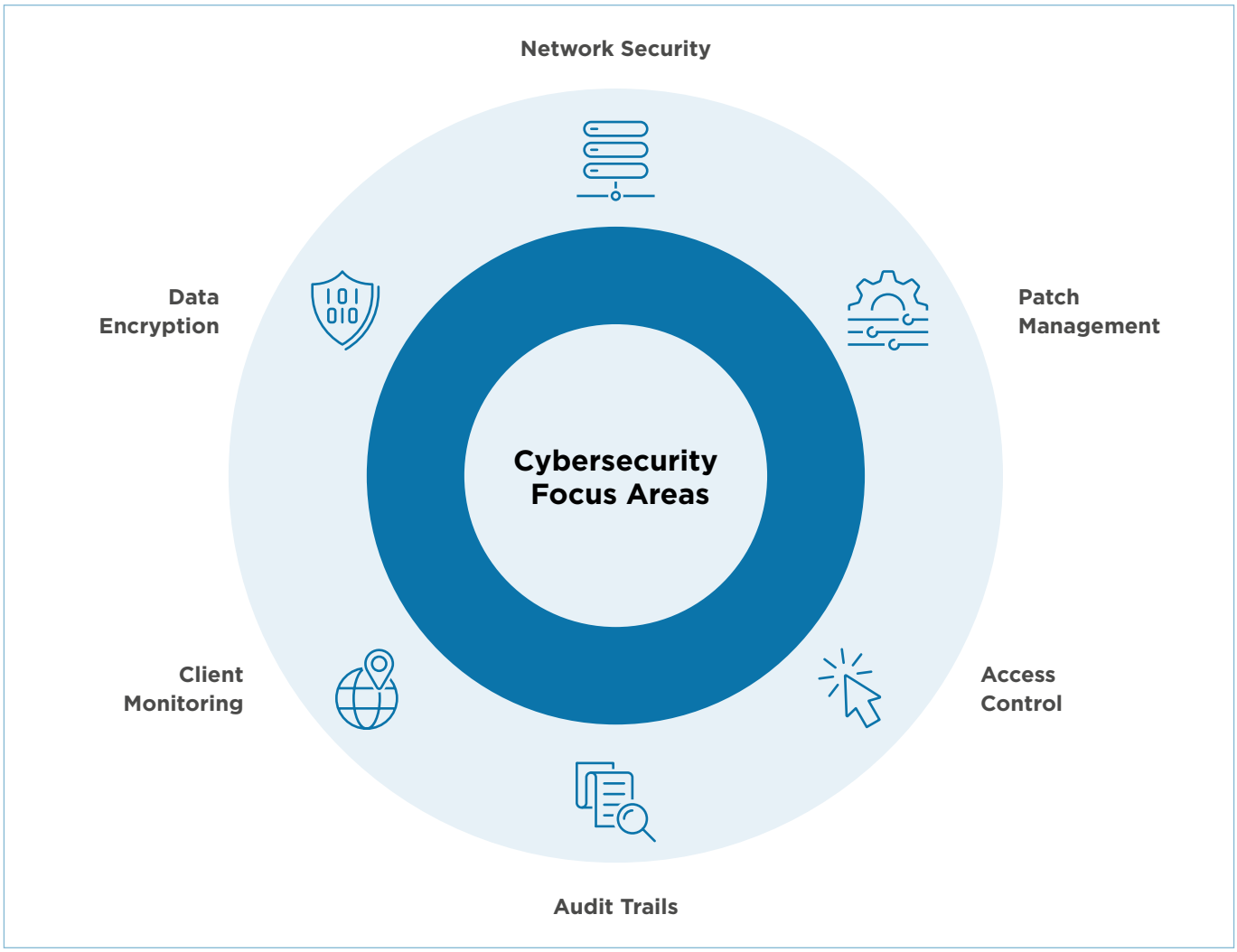
- poor software patch management and delayed software updates
- unqualified two-factor authentication methods
- weak encryption for sensitive data
- insufficient audit logging and negligible monitoring
- excessive user privileges without proper access controls.

2. Cybersecurity focus areas

SFC emphasized six core areas to improve security practices and operational safeguards (see diagram).

3. Emerging risks and recommendations

Firms must address legacy software, third-party



risk, and weak authentication to protect digital infrastructure:

- Address risks from end-of-life (EOL) software, unpatched virtual private network (VPNs), and phishing threats
- Strengthen third-party IT provider oversight and cloud security
- Replace SMS one-time passwords (OTPs) with biometrics or secure tokens.

4. Senior management responsibility

Senior management must lead cybersecurity risk management through oversight, governance, remediation, and contingency planning.

While compliance is expected immediately, a broader cybersecurity framework for all licensed corporations is planned for 2025 that would be beyond internet trading.

Challenges and action steps

While cyber breaches are inevitable, we believe firms can contain damage through preparedness. Some of the challenges that HK and Indian firms are likely to face will include low maturity in security testing, minimal exposure to vendor-managed cybersecurity platforms and high complexity of data encryption and privacy compliance. To overcome these challenges, firms should build red (ethical hackers) and blue (defender) teams, undergo vendor due diligence exercises to arrive at a best-fit, and rewire their existing data encryption and storage strategy.

Listed below are a few key workstreams that should be part of cybersecurity change programs:

- **Network micro-segmentation:** Restrict lateral movement of threats by dividing the network into isolated segments with granular access controls.
- **Legacy network protocol removal:** Eliminate outdated and vulnerable network protocols to reduce attack surfaces and enhance security posture.
- **Penetration testing:** Simulate cyberattacks on computer systems, networks, or web applications to identify and exploit vulnerabilities, helping to improve security.

How Capco can help

Capco supports financial institutions across APAC in strengthening their cybersecurity and cyber-resilience posture.

We bring a blend of **cyber-risk expertise, regulatory insight, and transformation delivery** capabilities, offering:

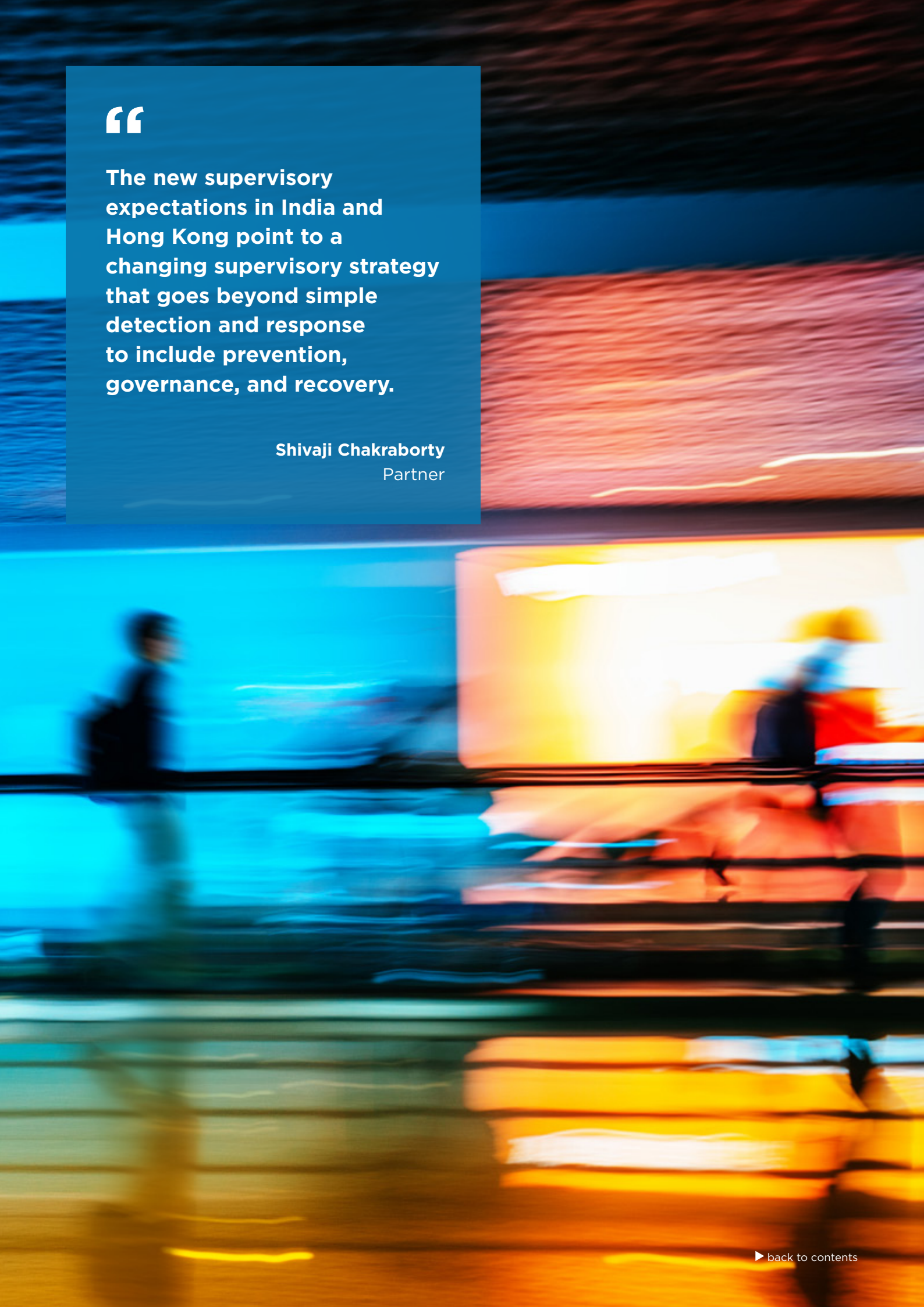
- **Gap assessments** aligned with IFSCA and SFC frameworks
- Design and implementation of **cybersecurity governance models**
- **Cyber-incident response playbooks** and simulations
- **Third-party risk management** and outsourcing control design
- Support in **policy creation**, VAPT vendor coordination, and board-level awareness programs.

Whether you're regulated by IFSCA, SFC, or other APAC supervisors, Capco helps ensure cybersecurity is a **strategic enabler**, not a reactive control.

Sources

https://ifsca.gov.in/Viewer?Path=Document%2FLegal%2Fguidelines-on-cyber-security-and-cyber-resilience-for-regulated-entities-in-ifscs-1-10032025064412.pdf&Title=Guidelines%20on%20Cyber%20Security%20and%20Cyber%20Resilience%20for%20Regulated%20Entities%20in%20IFSCs&Date=10%2F03%2F2025

https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=25EC7



The new supervisory expectations in India and Hong Kong point to a changing supervisory strategy that goes beyond simple detection and response to include prevention, governance, and recovery.

Shivaji Chakraborty
Partner

▶ back to contents

18. The Bank of Thailand raises the bar on high-risk transactions and sanctions exposure



Key Headlines

- In order to improve financial institutions' defences against transactions involving high-risk nations and risks associated with sanctions, the Bank of Thailand (BOT) and the Anti-Money Laundering Office (AMLO) have released a unified policy.
- Financial institutions are required to monitor for dual-use items (DUI) in transactions, confirm ultimate beneficial ownership (UBO), and do enhanced due diligence (EDD).
- To stop the Thai financial system from being used for illegal purposes, the policy highlights the necessity of strong governance frameworks, risk assessments, and compliance procedures.

Regulatory context and objectives

The BOT and AMLO have stepped up their supervision of financial institutions in response to growing international concerns about the proliferation of weapons of mass destruction, money laundering, and terrorism financing. There have been recent instances of financial institutions in Asia getting penalized for aiding transactions to sanctioned entities in Eastern Europe as well as Asia. This policy attempts to prevent Thailand's financial system from being used as a conduit for illegal activity and is in line with international standards established by the Financial Action Task Force (FATF). For Thai banks with regional as well as international aspirations, embedding the policy will be a competitive differentiator in cross-border expansion.

Key regulatory measures

1. **Enhanced customer due diligence (EDD)**
   Strict EDD procedures must be implemented by financial institutions, particularly for clients from high-risk nations. This comprises:
   - Extensive UBO verification using trustworthy, impartial sources
   - Thorough investigations into the intent behind transactions to guarantee conformity with stated corporate goals
   - Transactions are continuously checked for irregularities or warning signs.
2. **Sanctions risk management framework**
   Institutions need to create thorough systems for evaluating, tracking, and reducing the risks associated with punishments. Important elements include:
   - Regular risk evaluations that consider transaction types, geographic exposure, and consumer profiles
   - Installation of mechanisms to identify and notify of possible violations of sanctions

- Defining precise guidelines and practices for handling risks that have been identified.

3. Governance and oversight

The policy underscores the importance of strong governance structures:

- **Board of directors:** Responsible for setting, recommending, and approving policies, strategic plans, sound risk governance frameworks, and transactions that may involve significant sanctions-related measures with potential implications for the institution's operations and reputation.

- **Senior management:** Tasked with implementing sanctions-related risk management frameworks, including efficient processes, risk limits, clear reporting structures, and regular reviews to ensure compliance and timely detection of risks.

4. Monitoring dual-use items (DUI)

Financial institutions need to be on the lookout for transactions involving DUIs, i.e., items that have both civilian and military use. This comprises:

- Developing tools and systems to identify DUIs

- Establishing common high-priority lists (CHPLs) of issues that need closer examination in cooperation with trade associations.

For Thai banks with regional as well as international aspirations, embedding the policy will be a competitive differentiator in cross-border expansion.

Implementation timeline

Financial institutions must comply with the guidelines stipulated in the Joint Policy Statement from December 27, 2024 onwards. Enhanced standards to monitor dual-use items and high-risk products will be applied starting January 2025.





Implications for financial institutions

According to the joint policy, Thai financial institutions must:

- Include improved due diligence procedures for high-risk clients, guaranteeing thorough confirmation of UBOs and transaction objectives
- Create and put into place strong frameworks for managing the risk of sanctions, including frequent evaluations and conformity to international standards
- Establish industry-wide guidelines for tracking DUIs and high-risk products to stop money channels from being abused for illegal purposes.

Firms could face implementation challenges due to over dependency on manual processes, dynamically changing UBO sanction lists, and current infrastructure being inadequate for sanctions screening. They would need to review their current inventory of sanctions screening systems and upgrade the same for real-time and automated screening. Firms which invest in AI-supported transaction screening and automated UBO mapping will be able to onboard low-risk clients at speed and high-risk clients with precision. Access to global sanctions lists and integrating the data with the screening tools will be a success factor of the overall implementation. It is advisable to use case management systems for flagging suspicious cases and maintaining an audit log of all cases for BOT or AMLO inspection in future.

How Capco can help

Capco stands ready to assist financial institutions in navigating these enhanced regulatory requirements:

- **Risk assessment and framework development:** Designing and implementing comprehensive risk management frameworks tailored to the institution's specific needs.
- **Technology integration:** Implementing cutting-edge systems for DUI detection, sanctions screening, and transaction monitoring.
- **Training and capacity building:** Offering specialized training courses to make sure employees are prepared to manage new compliance requirements.
- **Assurance services:** Conducting independent reviews to assess the effectiveness of implemented measures and identify areas for improvement.

By leveraging Capco's expertise, financial institutions can improve operational resilience, guarantee regulatory compliance, and preserve the integrity of Thailand's financial system.

Sources

Joint Statement Enhancing Policies and Operational Guidelines of Financial Institutions Regarding Transactions with High-Risk Countries and Managing Sanctions-Related Risks

https://www.bot.or.th/content/dam/bot/fipcs/documents/FPG/2567/EngPDF/25670220.pdf

19. Integrity and security: OSFI's No.1 risk for 2025

Introduction

The Office of the Superintendent of Financial Institutions (OSFI) plays a key role in protecting the Canadian financial system. Following the passage of Bill C-47 in 2023, OSFI's mandate expanded to include oversight of integrity and security risks. In 2024, OSFI's Integrity and Security Guidelines came into effect, formalizing expectations for federally regulated financial institutions. According to OSFI's 2024-2025 Annual Risk Outlook, integrity and security is now its top supervisory priority, encompassing not only cyber threats, but also foreign interference, insider risk, and physical security. As of January 31, 2025, all federally regulated financial institutions are expected to be fully compliant with the new requirements.

This shift reflects the recognition that these risks now pose systemic threats to institutional stability and public trust. Integrity and security are no longer the sole responsibility of IT or compliance teams; they are enterprise-wide priorities requiring board oversight, integrated risk management, and clear accountability.

What is integrity and security in a financial context?

Integrity and security are defined as the safeguarding of systems, data, and digital infrastructure to ensure secure and ethical financial operations.

The **key components** of these guidelines include:

Security

1. **Secure technology and cyber defenses**
   - Implement controls to protect technology assets from cyber threats and malicious activity, including those managed by third-party providers.

2. **Protection of data and information**
   - Safeguard the confidentiality, integrity, and availability of data, with clear expectations on how sensitive information is handled and accessed.

3. **Security of premises and personnel**
   - Maintain physical security of facilities and apply risk-based screening and access controls for employees, contractors, and third-party partners.



Integrity

1. **Integrity of responsible persons**
   - Ensure individuals in sensitive roles, including external contractors, are of good character and subject to appropriate vetting and oversight.

2. **Culture of integrity**
   - Promote an enterprise-wide culture of ethical conduct, transparency, and personal accountability, reinforced through training and leadership tone.

3. **Oversight and compliance**
   - Maintain governance, compliance, and whistleblower systems to detect and respond to misconduct, including risks introduced through third-party relationships.

How do these guidelines compare with international regulations?

OSFI's move aligns Canada with global regulatory trends in operational resilience and governance. Below is a comparison of OSFI's key themes against the UK, EU, APAC and the US:

OSFI integrity and security themes versus global regulatory frameworks

OSFI Theme	UK	EU	APAC	USA
Security	• **PRA SS1/21** – Requires ICT and operational resilience • **NCSC Cyber Essentials** – Baseline cyber controls • **SYSC** – Safeguarding firm assets • Physical security included under operational risk expectations	• **DORA** – ICT risk management and cyber resilience (Articles 5–15) • **GDPR (Art. 32)** – Security of personal data (CIA) • **NIS2 Directive** – ICT and physical risk protection for critical sectors	• **MAS TRM Guidelines** – Cyber controls, data and system security • **APRA CPS 234** – Information security and third-party accountability • **PDPA / HKMA TM-G-1** – Data and facility protection	• **NIST CSF** – Industry-standard cyber risk framework • **GLBA Safeguards Rule** – Customer data protection • **FFIEC IT Handbook** – Cybersecurity and tech governance • **Bank Protection Act** – Physical security for facilities
Integrity	• **SMCR** – Personal accountability and fit-and-proper standards • **UK Corporate Governance Code** – Ethical leadership and conduct • **SYSC 6** – Compliance oversight requirements	• **CRD V / CRD IV** – Fit-and-proper (Art. 91) • **EBA Internal Governance Guidelines** – Conduct and oversight • **EU Whistleblower Directive** – Internal reporting channels required	• **MAS Fit & Proper Guidelines** – Vetting and conduct standards • **APRA CPS 220/520** – Culture, governance, and accountability • **HKMA Culture Reform** – Conduct expectations and monitoring	• **OCC Heightened Standards** – Ethical culture and board oversight • **FDIA §19** – Bars individuals with dishonesty-related convictions • **SOX Section 404** – Internal control and compliance frameworks

OSFI's I&S Guideline is new (2024) and brings Canada in line with international norms. The EU's DORA (2023) and the US interagency Third-Party Guidance (2023) are recent responses to digital risk and outsourcing risk, and the UK's SMCR (2016) is a more established regime on conduct. All share a common path: raising the bar for non-financial risk management and ensuring financial institutions are better governed and more resilient.

Looking ahead

To address the current landscape, OSFI expects federally regulated financial institutions (FRFIs) to:

- **Implement all components of OSFI's Guidelines B-13, B-10, E-21, and B-15** as part of an interconnected operational risk strategy
- **Strengthen enterprise-wide risk management frameworks** by embedding integrity into the management of operational, technology, and third-party risk
- **Expand background screening protocols** for a broader scope of personnel beyond exclusively senior roles



- **Report to OSFI without delay** about any incidents reported to law enforcement or intelligence agencies in a timely fashion
- **Strengthen physical security controls**, such as access management, facility protection and surveillance, to protect critical infrastructure and data
- **Apply integrity and security standards to third-party providers**, ensuring controls are consistent with internal expectations.

Beyond technical and operational controls, OSFI expects business leaders to embed ethical and security principles across the enterprise. This includes:

- **Embedding security and ethics into governance structures** to establish clear accountabilities, and using the three lines of defense model to reinforce across business, risk, and enterprise functions
- **Investing in cybersecurity tools, talent, and threat intelligence capabilities** to build resilience and cyber capabilities

OSFI's move aligns Canada with global regulatory trends in operational resilience and governance.

- **Fostering a risk-aware and ethical culture** starting with board and senior management and reinforced through conduct policies, training and organizational values.

Implementation timelines

The phased implementation approach will be finalized in 2025:

JUL 31, 2024

Submit a comprehensive action plan for OSFI's review, on new and expanded expectations, which includes interim deliverables to achieve compliance.

JAN 31, 2025

Observe all new or expanded expectations except on background checks.

JUL 31, 2025

Observe new expectations on background checks.

How Capco can help

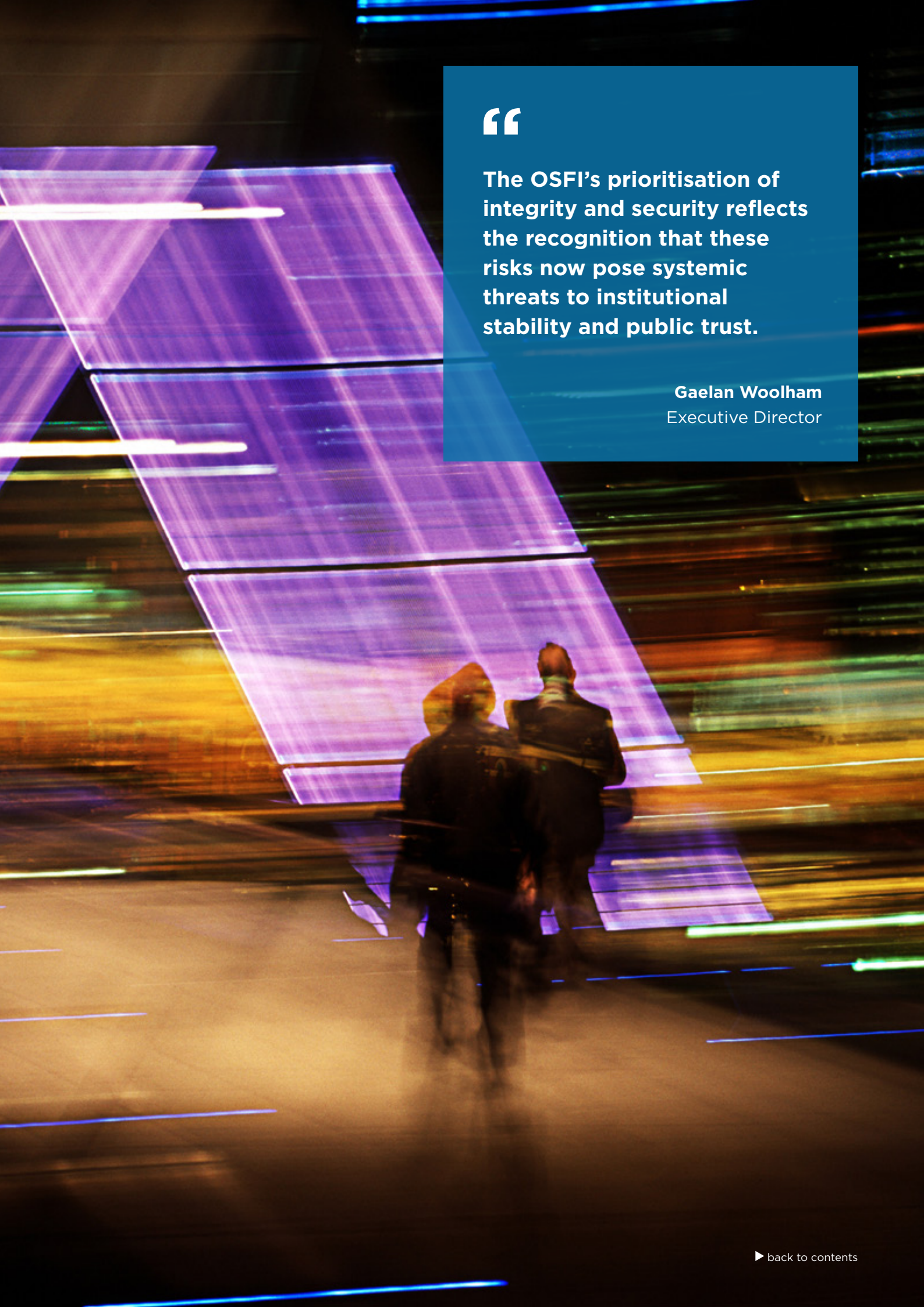
This Guideline signals a significant shift to a more holistic and rigorous oversight of non-financial risks. Leaders should take this opportunity to strengthen their foundations, starting by conducting enterprise-wide risk assessments against the new principles, updating policies, delivering training sessions, and investing in improved controls. It's also crucial to establish clear ownership to drive the implementation.

As a global consulting firm with deep experience in financial risk and regulatory compliance, Capco can help FRFIs navigate these changes through enhancing areas of:

- **Cyber-risk management:** Designing and implementing robust cybersecurity frameworks and controls, conducting maturity assessments against industry standards, and enhancing incident response plans.
- **Insider risk and culture:** Developing comprehensive insider threat programs and strengthening governance around conduct risk. This can include improving background check processes, establishing ongoing monitoring and aligning practices with global best-in-class regimes.
- **Third-party risk:** Assessing and upgrading TPRM programs to incorporate integrity and security criteria, for example, refining due diligence checklists to include cyber and geopolitical risk factors, and updating contracts and oversight routines. Capco can also benchmark your practices against the new OSFI B-10 expectations and US/EU standards.
- **Regulatory change readiness:** Providing program management and advisory support to ensure a smooth implementation of the guideline. This includes helping draft the OSFI action plan, mapping out responsibilities and timelines, training executives and boards, and building dashboards to track progress, all the while bringing experience from similar global regulatory initiatives.

By embracing OSFI's enhanced expectations and partnering with Capco to carefully plan and navigate the landscape, financial institutions will not only satisfy regulatory requirements but also build greater operational resilience and trust with stakeholders, emerging stronger, safer, and more resilient.





> **The OSFI's prioritisation of integrity and security reflects the recognition that these risks now pose systemic threats to institutional stability and public trust.**
>
> **Gaelan Woolham**
> Executive Director

▶ back to contents

20. Financial Data Access regulation (FiDA)



Key Headlines

- FiDA is set to revolutionize the financial sector by expanding data-sharing frameworks
- Adoption is expected in 2025, with transitional periods until the implementation phase, which will likely start in 2027.
- The road ahead may be challenging, but the rewards – for both institutions and consumers – are well worth the effort.
- As FiDA takes shape, it promises to redefine how financial data is shared and utilized, driving a new era of transparency, innovation, and consumer empowerment
- For businesses, FiDA will bring opportunities for innovation in product offerings and new partnerships between traditional firms and fintechs.

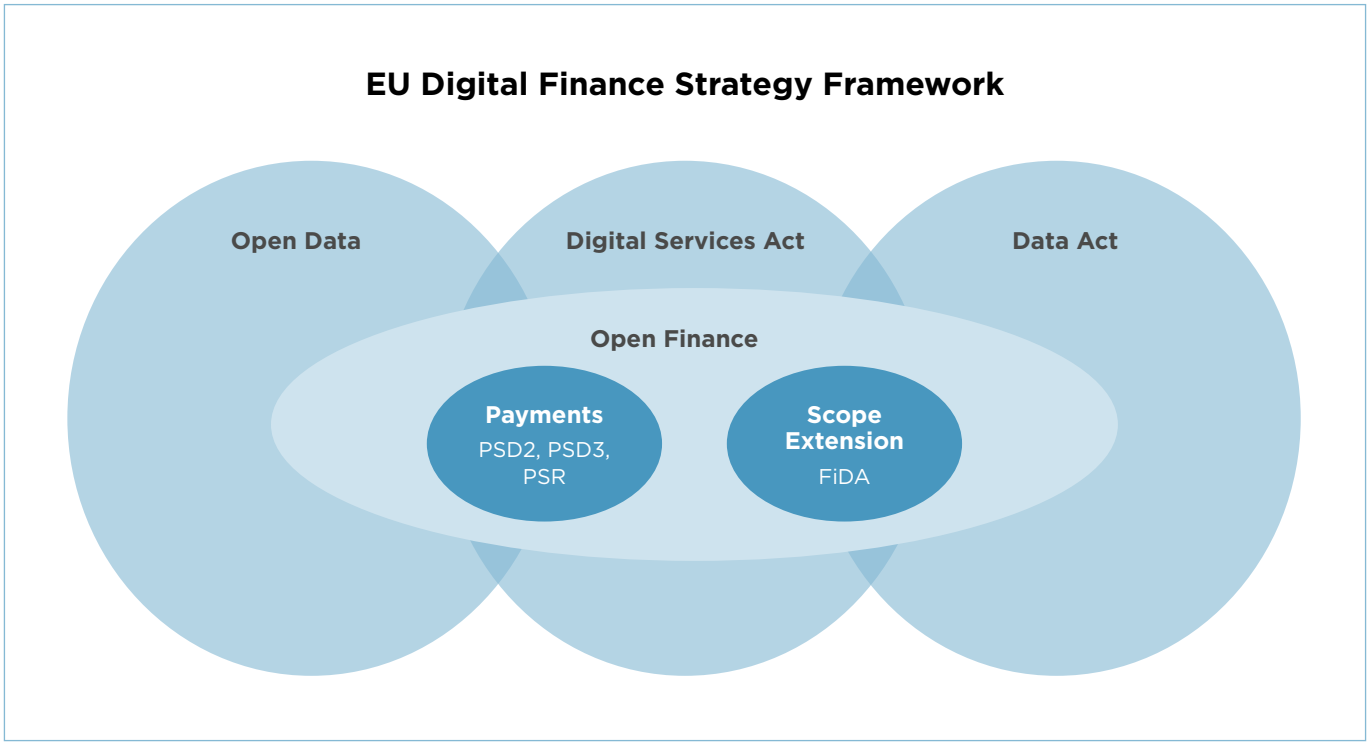
In December 2024, the EU Council reached an agreement on a proposed framework for access to financial data (FiDA). In its position, the Council largely supports the Commission's original proposal and is pursuing a gradual approach to implementing the regulation. The FiDA regulation is currently under review by the European Parliament and the Council of the European Union. Adoption is expected in 2025, with transitional periods to allow businesses and regulators to adapt to the new framework. The first implementation phase will likely start in 2027.

What is FiDA?

The FiDA regulation builds on the success of the Payment Services Directive 2 (PSD2), which introduced open banking in Europe, and its further evolutions of PSD3 and PSR. While PSD3 and PSR focus on payment services, FiDA expands the principles of data sharing to a broader range of financial products and services, including investment, insurance, pensions, and more. The regulation is designed to enable secure, efficient, and consumer-controlled access to financial data across the EU.

FiDA is part of a broader regulatory framework aimed at modernizing Europe's financial landscape. Key intersections include:

- **PSD2, PSD3, PSR:** FiDA builds on the PSD2, PSD3, and PSR open banking framework, expanding its principles to encompass all financial sectors.
- **GDPR (General Data Protection Regulation):** Aligns with GDPR's robust data protection standards to ensure lawful and secure data processing.
- **MiCA (Markets in Crypto-Assets Regulation):** Complements regulatory initiatives in digital assets, creating a holistic approach to digital finance.



Key objectives

FiDA aims to:

- **Enhance data sharing:** Facilitate safe and efficient data sharing across financial sectors, enabling new business models and innovative services.
- **Empower consumers:** Provide individuals and businesses with greater control over their financial data, ensuring they can easily grant, manage, and revoke access.
- **Strengthen competition:** Level the playing field by enabling market entry for fintech and third-party providers.
- **Ensure security:** Introduce robust safeguards to protect privacy and prevent misuse of financial data.

Core features of the regulation

Broader scope

- Covers data from a wide array of financial services, such as banking, investments, insurance, and pensions, impacting the whole financial industry (banks, insurance companies, wealth and asset managers, credit providers, etc.).
- Includes both financial institutions and non-bank providers, fostering a comprehensive open finance ecosystem.

Consumer rights

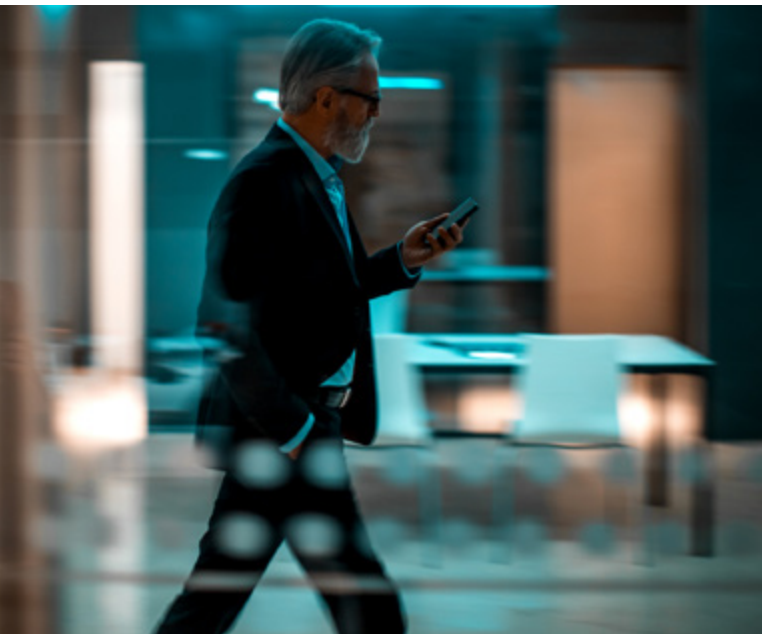
- Ensures consumers can easily manage their data-sharing preferences through standardized interfaces.

FiDA expands the principles of data sharing to a broader range of financial products and services, including investment, insurance, pensions, and more.

- Establishes the right to real-time access to machine-readable financial data and introduces a real-time financial data access permission dashboard.

Technical standards

- Introduces harmonized application programming interface (API) standards for secure and seamless data transfer.



- Standards will be developed in collaboration with entities like the European Banking Authority (EBA).

Governance and oversight

- National regulators and the European Commission will oversee compliance.

- Penalties for non-compliance will ensure adherence by data holders and third-party providers.

Interoperability and innovation

- Supports the development of advanced financial services, such as robo-advisors and personalized analytics.

- Encourages partnerships between traditional financial institutions and fintech companies.

What should firms do?

Legacy systems and their lack of interoperability will present the biggest hurdle for financial institutions when it comes to integrating new technical standards defined by FiDA. Upgrading these systems can be costly and time-consuming and potentially lead to delays in compliance. Financial Institutions should adopt an end-to-end approach, from designing and implementing compliant APIs to integrating them with existing systems. Scalable, cloud-based solutions can reduce costs and improve efficiency, ensuring a seamless transition to FiDA compliance.

Further challenges may arise from the varying interpretations of the regulation at the national level, leading to inconsistencies and added complexity in cross-border operations. Existing data structures should be mapped to FiDA-compliant standards and tools for data transformation should be used. Adopting industry-wide standards, like ISO 20022, will ensure interoperability and future proofing of existing systems.

Financial institutions may also encounter increased competition from agile fintech firms and will require significant investments in innovation to remain competitive. Financial institutions should develop innovative products and services that leverage open finance data. Strategic partnerships with fintechs can help to enhance offerings and create unique value propositions that set financial institutions apart from competitors.

In addition, developing new products that comply with FiDA can require substantial resources, and established institutions may need to rethink their strategies to stay competitive.

How Capco can help

Navigating the complexities of FiDA requires a strategic, holistic approach. We can support financial institutions with:

- **Regulatory expertise:** Providing deep insights into FiDA requirements and helping financial institutions to identify their impact and implement them effectively.

- **Technical implementation:** From API development to system integration, Capco offers end-to-end technical support to ensure compliance.

- **Change management:** Capco assists in managing organizational change, from training staff to redesigning business processes.

- **Innovation and strategy:** Capco identifies opportunities for innovation and helps institutions stay competitive in the open finance era.

21. India's Digital Personal Data Protection Act (DPDPA): Impact on the financial sector

With the release in January of its draft Digital Personal Data Protection (DPDP) rules, India's Ministry of Electronics and Information Technology (MeitY) has initiated the next step in the ongoing evolution of the nation's data protection framework. With a subsequent public consultation having closed in early March, we explore the implications for India's financial services industry and some key priorities for firms as they seek alignment with the new guidelines.



Emphasizing transparency, accountability, and lawful processing of digital personal data, the new rules serve as an extension of India's groundbreaking Digital Personal Data Protection Act, 2023 (DPDPA), and provide much-needed clarity on the Act's implementation. Shaping how businesses should collect, process, and safeguard personal data in the digital age, they mark a significant milestone in India's data protection journey.

The DPDPA introduced key principles such as principle of consent, purpose limitation, data minimization, personal data accuracy, storage limitation, data safeguard, and principle of accountability, aligning with global standards like the GDPR while incorporating India-specific regulatory nuances.

In the intervening period the regulatory landscape has continued to evolve, and the latest draft DPDP rules introduce several refinements to enhance compliance and implementation, including granular consent mechanisms, enhanced transparency on data usage, and sector-specific compliance adjustments tailored for industries like finance.

For financial institutions and fintechs, which rely heavily on digital data, this all marks a critical shift, and understanding and adhering to these new regulations will be critical to maintaining consumer trust, regulatory compliance, and mitigating legal and financial risks.

Impact on financial institutions and fintechs

The implications are far-reaching. Financial institutions must now be transparent about how they collect and use customer data, with explicit consent required at every touchpoint. Sensitive data – like financial information and medical records – will demand heightened protection and customers will have more control over their personal data, including rights to access, correct, delete, and restrict its processing.

Operationally, this affects areas such as customer onboarding, where clear and informed consent must be obtained. Risk profiling and marketing will need to be conducted with privacy in mind, and institutions must ensure customers can easily opt out of any data use. Customer service departments, too, must be ready to handle requests related to data correction or deletion efficiently.

Data retention policies will need to be re-evaluated to ensure personal data is only stored as long as

necessary. From a security standpoint, financial institutions must adopt technical and organizational safeguards to prevent data breaches or unauthorized use.

For fintechs, particularly startups and digital-first companies, the road ahead may be more challenging. As data processors work under regulated entities (REs), they'll face increased scrutiny and will need to build more mature data governance systems. Fintechs will have to map the data they handle, enforce purpose limitation, ensure compliance with cross-border data transfer norms, and possibly appoint data protection officers (DPOs) if classified as significant data fiduciaries.

Those fintechs that invest early and effectively in data governance will likely become preferred partners in the financial ecosystem.

Despite some concerns from the industry, the Act is a strong move towards strengthening India's digital infrastructure and could influence global privacy frameworks, thanks to unique features like algorithmic accountability, verifiable parental consent, and tighter controls on cross-border data transfers.



Navigating the new compliance landscape

To address the challenges ahead, financial institutions must focus on:

- **Data inventory and mapping:** Understand the type and flow of personal data
- **Consent management:** Implement clear, user-friendly consent processes
- **Data localization:** Comply with residency and transfer requirements
- **Cybersecurity:** Invest in infrastructure to prevent breaches.

We propose a three-step framework to help financial organizations navigate the DPDPA effectively:

Assess and strategize

- Conduct gap and risk assessments
- Align regulatory goals with business operations
- Develop a customized compliance roadmap.

Implement and govern

- Set up governance frameworks
- Deploy technical safeguards like encryption and access control
- Establish internal audit and risk monitoring mechanisms.

Communicate and sustain

- Train employees and vendors on data protection
- Launch awareness campaigns
- Engage stakeholders continuously to adapt to evolving rules.

Key priorities should also include developing comprehensive privacy policies, conducting regular privacy audits, ensuring vendor compliance, and creating a robust breach response strategy led by DPOs.

The DPDPA is a catalyst for cultural change in how organizations view and handle data. While compliance will require effort and investment, it also presents an opportunity to build stronger customer trust, improve data governance, and position Indian financial institutions as global leaders in privacy-first innovation.



Shaping how businesses should collect, process, and safeguard personal data in the digital age, the new DPDPA rules mark a significant milestone in India's data protection journey.

Gaurav Mehra
Partner

▶ back to contents

22. The future of regulatory reporting for financial institutions: An oversight on the Integrated Reporting Framework (IReF) and the Banks' Integrated Reporting Dictionary (BIRD)

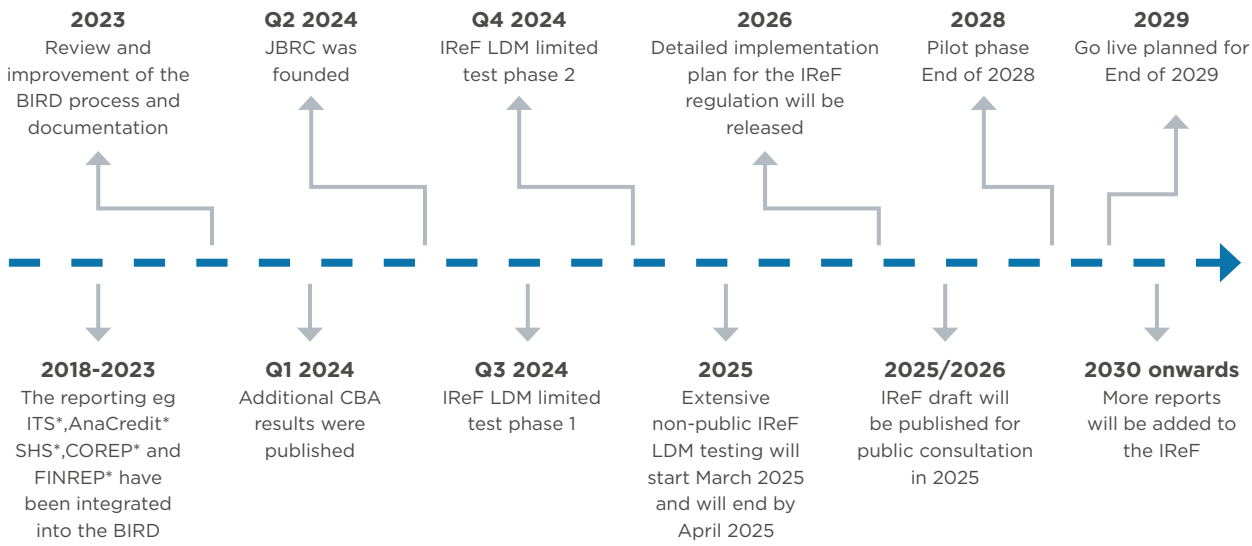
The European Central Bank (ECB) plans to implement the Integrated Reporting Framework (IReF) by the end of 2029, with the objective of harmonizing the production of regulatory data and alleviating the reporting burden on financial institutions. In support of the IReF roadmap (see timeline below), the ECB has also proposed the Banks' Integrated Reporting Dictionary (BIRD), a comprehensive data dictionary designed to facilitate consistent and efficient reporting. Financial institutions are advised to proactively prepare for the forthcoming regulatory developments, particularly in relation to ESG considerations and the integration of non-financial data.

The Integrated Reporting Framework (IReF)

IReF is a mandatory regulation designed to streamline regulatory reporting by consolidating existing reports into a single, unified framework. Its goal is to enhance efficiency across the financial service sector. IReF will establish uniformity in data definitions, reporting frequencies, and formats, ensuring consistency for financial institutions operating across multiple jurisdictions. Through standardized policies, IReF aims to improve the accuracy and reliability of reported data covered in existing regulations including AnaCredit, BSI, MIR, and SHS. The framework is supported by BIRD, which complements the IReF implementation by providing a standardized and harmonized data model that supports consistent generation of covered regulatory

The ECB plans to implement the Integrated Reporting Framework by the end of 2029.

The ECB plans to deploy the IReF by end of 2029



[i] The IReF roadmap follows a phased timeline toward full implementation by end of 2029, with key milestones including technical preparation, pilot testing, and gradual integration of reporting standards.

reports. Overall, IReF seeks to enhance transparency and regulatory compliance within the financial service industry.

The Banks' Integrated Reporting Dictionary (BIRD) framework

BIRD is a foundational technology for IReF, developed in a collaborative initiative between the ECB and the financial service industry. BIRD is currently voluntary, however, due to its connection to the regulatory required IReF, its adoption is strongly encouraged as it facilitates a smoother transition and ensures compliance with future regulatory standards.

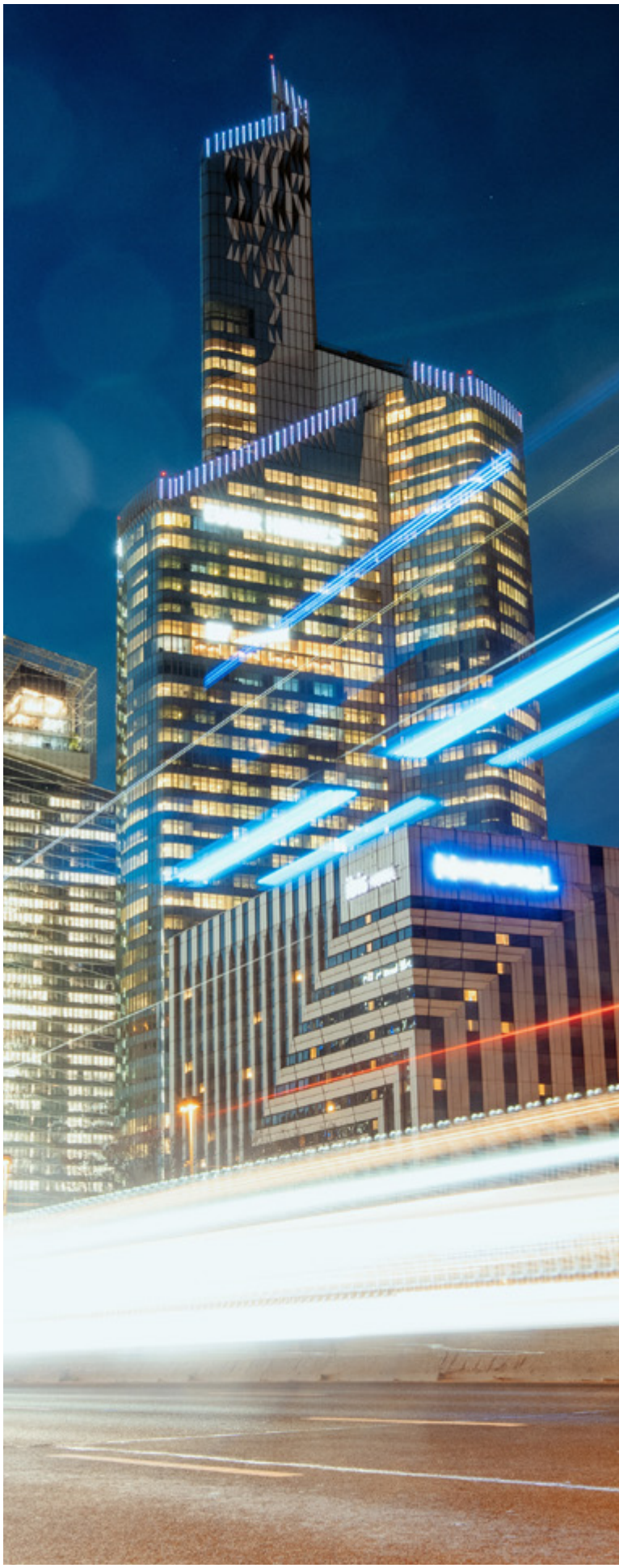
It provides a harmonized data dictionary, data model, and transformation rules based on best practices. BIRD specifies how data should be extracted from the internal IT systems and transformed to generate the reports required by authorities. The initiative aims to reduce the reporting burden by offering standardized, unambiguous definitions of reporting concepts and facilitates an industry-wide consistent reporting. It is important to note that BIRD is not an IT tool or regulatory act, and it does not introduce new regulatory requirements, but rather it enhances existing reporting processes.

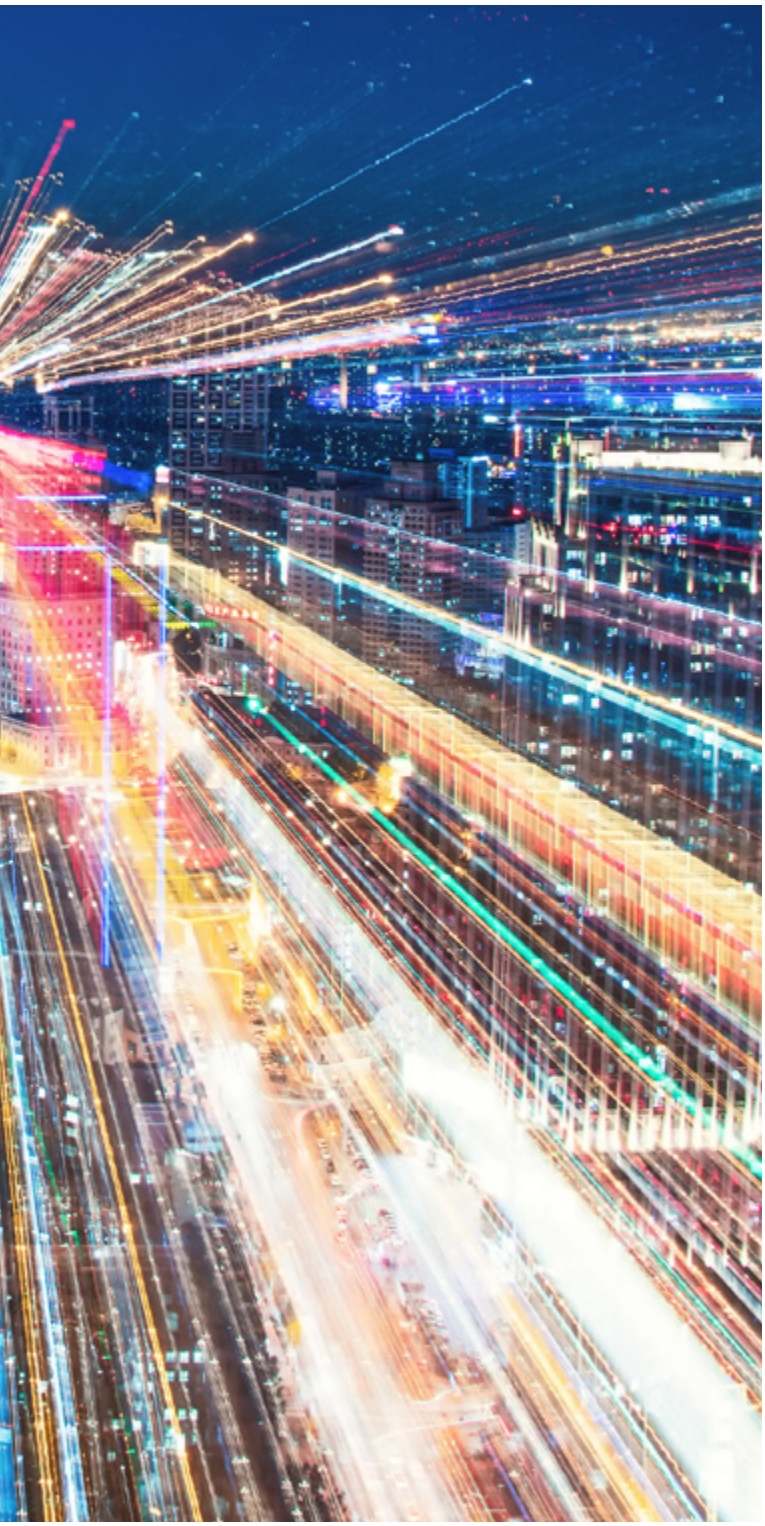
Transitioning to BIRD can be complex, but modern tools like AI can streamline the process by automatically translating and mapping existing internal regulatory data dictionary to BIRD's standardized framework. This approach greatly reduces manual workload and helps minimize the risk of misinterpretation.

IReF, BIRD, BCBS 239 and data management need to be considered jointly

The BIRD-based IReF rollout introduces a range of challenges that must be addressed in alignment with BCBS 239 compliance, DORA, and broader data management reforms. While IReF aims to harmonize statistical reporting across the Eurozone through a standardized input layer, its success hinges on a unified, enterprise-wide data strategy within financial institutions.

A key challenge is data standardization within each financial institution. IReF demands consistent data definitions and structures that align closely with BCBS 239's principles for effective risk data aggregation and reporting. However, outdated legacy systems, fragmented architectures, and siloed business lines





often obstruct the creation and maintenance of a common data model or even a common data layer, a cornerstone for both regulatory compliance and operational efficiency.

In parallel, the increasing emphasis on digital resilience under DORA places further demands on institutions to ensure their data infrastructure is not only compliant but resilient to disruption. This includes robust data lineage, complete audit trails, and integrated governance frameworks that can withstand regulatory scrutiny and operational stress scenarios.

Meeting these challenges requires a coordinated, organization-wide approach to data management. This approach must bridge regulatory compliance with scalable operational practices, fostering a cohesive environment that enhances data lineage, data quality, operational efficiency, risk management, and digital resilience across the financial sector.

Obstacles in the IReF and BIRD implementation

IReF represents a significant step forward in the ECB's efforts to streamline and enhance the quality of regulatory reporting across the euro area. IReF is designed to support a harmonized reporting system that enables better decision making while also reducing the long-term reporting burden on institutions.

To meet the objectives of IReF, financial institutions will need to invest in robust data infrastructure, align internal data governance processes, and ensure that their reporting systems can deliver high-quality, granular data in line with the IReF's requirements. This transition demands strategic planning, cross-functional coordination, and early engagement with implementation guidelines and testing phases to ensure readiness ahead of IReF's anticipated rollout.

How Capco can help

Our cross-functional team leverages proven expertise in data management, risk management, and regulatory compliance to perform a thorough evaluation of the existing client solution. Our successfully proven approach, based on best practices, ensures a seamless transition to compliant and agile reporting mechanisms and addresses both the technical and business aspects to develop data-driven strategies and implement a data management framework. Capco offers a strategic roadmap for building strong governance frameworks and addressing future challenges, helping clients reduce regulatory pressure and optimize compliance reporting.

Financial Crime

▶ back to contents

23. Role of technology in financial crime prevention: FCA's perspective and industry innovations

Financial crime (FinCrime) compliance, due to the volume of work, the evolving threat landscape, and the risk of getting things wrong, has led to the increasing uptake of technology within the financial services industry. As the adoption of technology has been dramatically increasing, the FCA's understanding of technological benefits has also been evolving, whereby they have adopted the position of encouraging firms to explore them. As a result, adoption and improvements to FinCrime technology will continue to be a strong trend within the industry.

FCA perspective

The FCA's support of a technology and data-driven approach to combatting FinCrime has been outlined across its various initiatives, such as the Financial Crime Guide and the Regulatory Sandbox.

Firms are encouraged to:

- Use technology in onboarding, name screening, and data analytics to identify risks
- Balance manual oversight with automated processes for a comprehensive risk view
- Regularly test systems and understand their capabilities, limitations, and risks
- Justify the logic behind automation (e.g., triaging, machine learning, alert suppression)
- Calibrate and tailor tools to the firm's specific risk profile and operational needs
- Leverage automation for high-volume transaction processing
- Document reasons for deactivating or decommissioning systems or rules, and ensure contingency measures are in place.

Industry innovations

The extent to which firms have been adopting technologies varies, with some adding capabilities to existing systems, such as enhanced fuzzy logic for screening systems or visual trends analysis for management information (MI), whilst others are building full solution platforms based on artificial intelligence (AI) and machine learning (ML).

AI, ML and generative AI: AI and ML are being deployed for transaction monitoring, filtering, and name screening to analyze large datasets, identify patterns, and distinguish true alerts from false positives. False positives are a key operational issue facing the industry for TM (transaction monitoring), where many firms are actively looking to utilize ML to increase the SAR conversion ratio. Generative AI (GenAI) is another emerging transformative tool being used for synthesizing data across multiple systems to generate contextual narratives for alerts, assist in drafting risk reports / SARs and automate repetitive documentation processes. When embedded within compliance workflows, GenAI enhances decision making, reduces human error, and allows analysts to focus on complex risks.

Smart know your customer (KYC): Next generation KYC technologies include facial and voice recognition, behavioral biometrics, and e-KYC platforms that enhance the accuracy of identity verification. These innovations strengthen compliance and transform the customer onboarding journeys by minimizing friction and reducing processing times. In addition, firms are implementing case management platforms with integration into these next generation technologies to enhance KYC workflows and monitor identity changes.

Intelligent alert triage and decisioning engines: Firms are integrating AI-powered decisioning engines into their FinCrime ecosystems. These tools go beyond traditional case management by applying intelligent logic to automatically assess alert relevance, recommend actions, and escalate only high-risk cases to investigators.

Real-time risk intelligence platforms: Modern FinCrime teams are moving away from periodic assessments to continuous risk monitoring through real-time risk intelligence platforms. These systems aggregate internal and external data feeds, including



KYC, TM, sanctions, and geopolitical data into a dynamic risk model that evolves as new threats emerge. This shift enables proactive risk identification and mitigation, tailored to both customer and business risk profiles.

Dynamic dashboards: Data from dynamic risk assessments are being utilized to produce MI through visual dashboards. These dashboards allow various stakeholders to monitor and address real-time risk, as opposed to traditionally static reports consisting of retrospective data. Additionally, some MI dashboards are developed to provide insights on historical data and generate predictive trend analyses.

Case study

Capco helped a Tier 1 global bank overcome significant challenges in its call center operations, particularly in managing fraud-related customer calls. Capco's implementation of an AI powered call summarization assistance tool transformed how the bank's agents handled fraud-related calls, leveraging advanced transcription and summarization technology to transcribe live conversations and extract critical information for analysis. The solution proved to be transformative, with a senior client stakeholder describing it as "a significant breakthrough" in addressing operational inefficiencies and improving fraud call handling.

How Capco can help

At Capco, we specialize in delivering end-to-end FinCrime transformation and implementation projects. Our team has deep expertise in supporting clients across a range of areas, including dynamic risk assessments, vendor selection, TM system implementation, screening calibration, and deployment of KYC case management tools. Through strategic partnerships with leading technology vendors, we help accelerate transformation initiatives and have also supported clients in designing bespoke in-house solutions tailored to their needs.

Technology can be adept at helping streamline and expedite otherwise manual processes. However, there should always be a human element involved to action items and have systems oversight, so that the efficiency of technology can be complemented by the contextual understanding of staff. We have an extensive understanding of the risks involved with embedding various technologies into FinCrime processes and can manage them in a way that allows clients to adopt technology with confidence.

24. Economic Crime & Corporate Transparency Act

Introduction

The act is a wider-reaching follow up to the 2022 Economic Crime Transparency and Enforcement (ECTE) 2022 Act that was designed to crack down on illicit money in the UK economy in the aftermath of the Russian invasion of Ukraine. The new ECCTA focuses on **increasing transparency of company registration** to make it harder for criminals and OCGs (organized crime groups) to launder money or commit fraud, along with a requirement for in-scope large organizations **to have adequate anti-fraud procedures in place** (the new Failure to Prevent Fraud (FtPF) offense). The FtPF will also encourage more organizations to implement or improve prevention procedures, driving a major shift in corporate culture to help prevent fraud.[27]

Timeline

ECCTA received royal assent on **26 October 2023**, with significant sections coming into effect throughout 2025:

- **March 2025: Companies House reform** to improve transparency of company registration to make it harder for foreign criminal gangs to launder money or commit fraud.

- **September 2025: New requirements** for large in-scope companies **to have adequate anti-fraud** measures in place. The new FtPF offense comes into force on September 1, 2025. Under this new offense, a **company will be criminally liable** for the offense if a person associated with it commits fraud with the intention of benefiting the organization (or any customer for which the associate provides services on the organization's behalf), and the organization did not have reasonable fraud prevention procedures in place. The offense is **punishable by an unlimited fine**[28].

Failure to Prevent Fraud

ECCTA focuses on preventing abuse of the UK's corporate structures and ultimately on reducing Financial Crime. As the **FtPF offense** comes into force on **September 1, 2025**, we expect all in-scope organizations to have plans and activities underway to prepare and strengthen their anti-fraud framework.

FtPF impacts large organizations, defined as meeting two out of three prerequisites:

- 250+ employees
- 336m+ in turnover
- 18m+ in assets.

Where prosecuted, an organization **will be required to demonstrate that it had reasonable fraud prevention measures** in place at the time that the fraud was committed; it is intended that FtPF will encourage and **assist organizations in the creation of an anti-fraud culture**.



27. Guidance to organisations on the offence of failure to prevent fraud
28. Failure to prevent fraud: how to prepare for new UK corporate offence - BM Insights - Blake Morgan

What should be done by September 1, 2025?

The FCA have detailed six specific principles, as shown below:[29]



1. **Risk assessment:** assessing perceived risks of associated persons committing a fraud offense. It should be noted that there is **no absolute requirement for organizations to do anything new** or different in approach or frequence for FtPF, however, the risk assessment should be **proportionate to the organization's size, nature and complexity, and should be documented and kept up to date**.

2. **Risk-based prevention policy and procedures:** perform a review of fraud prevention procedures. On completion of risk assessment and review of existing fraud prevention procedures, the organization may view that the risks are **sufficiently mitigated** through existing controls. Any conclusion should be **kept under periodic review to assess if procedures in place continue to be reasonable in relation to the risk they face** at that time.

3. **Due diligence:** an additional form of fraud risk assessment (see Principle 1). Recommended that **due diligence be applied on a risk-sensitive basis**. Companies should also consider having procedures in place that prevent "associated persons" who have been exited due to FtPF-related concerns from being re-onboarded.

4. **Communication:** training and awareness for senior leadership, employees or agents, and subsidiaries, should be designed to comply with FCA expectations.

The new ECCTA focuses on increasing transparency of company registration.

29. UK Finance Failure to Prevent Fraud Guidance, UK Finance Failure to Prevent Fraud industry guidance.pdf



Whistleblowing channels should be clearly described, with process and procedures available to all employees or agents.

5. **Monitoring and review:** required to ensure fraud framework effectiveness is monitored. Regular review of the fraud risk assessment, fraud prevention, and due diligence procedures should be conducted with outcomes reported to management for oversight and visibility.

6. **Top-level commitment:** ensuring senior managers are responsible for setting an example, displaying appropriate "tone from the top." The senior (executive) managers may issue communications stating commitment to the prevention of "associated persons" of the organization committing a fraud offense[30].

How Capco can help

Capco consulting can guide your organization through ECCTA and FtPF readiness activities, focusing efforts on the six key principles defined by the FCA, while providing delivery skills to ensure a timely implementation.

Checklist of Key FtPF readiness activities

✓ Perform and document the Fraud Risk Assessment.

✓ Review your Fraud prevention procedures, ensuring the outcome of the review is documented.

✓ Ensure senior management understand ECCTA and FtPF requirements, setting a commitment statement.

✓ Perform a detailed review of Due Diligence procedures.

✓ Ensure regular review of the fraud risk assessment, fraud prevention and due diligence procedures (consider creation of a control, supporting KRI for management oversight and visibility).

The new Failure to Prevent Fraud offense will encourage more organizations to implement or improve prevention procedures.

✓ Ensure Legal, Compliance, Financial Crime, Supplier Management, Finance, Relationships Management, Training and all other key departments receive targeted enhanced training, along with ECCTA awareness training for all staff.

30. UK Finance Failure to Prevent Fraud Guidance, UK Finance Failure to Prevent Fraud industry guidance.pdf

25. Navigating the storm: Sanctions risks under the Trump administration



Picking up where his first term left off, the 2025 Trump administration's foreign policy has re-emphasized the use of economic sanctions, creating a dynamic and often unpredictable risk environment for financial institutions. Sanctions became a central tool of statecraft, applied not just to traditional adversaries but increasingly to strategic rivals, individuals, and companies worldwide. As the US enters a new phase of leadership under Trump, banks must reassess their operational readiness and compliance frameworks to keep pace with rapid regulatory developments.

From "maximum pressure" to market disruption

The Trump administration's "maximum pressure" campaigns transformed sanctions from focused diplomatic levers into sweeping instruments of economic isolation. President Trump's second term has ushered in significant shifts in US sanctions policy, impacting financial institutions worldwide.

Specifically, this approach has included:

- Tightening sanctions on Russian financial and energy industries.
- Increasing the number of Chinese entities and individuals under various sanctions programs. Further, Trump has increased tariffs on China and issued a presidential memorandum to significantly review and eliminate loopholes in export controls for Chinese trade with a focus on curbing China's role in Fentanyl trafficking.

- Issuing new sanctions and export controls on Iran, including calling on the Treasury Department to consider imposing "Know Your Customer's Customer" obligations with respect to Iran-related transactions and to assess beneficial ownership thresholds to ensure sanctions "deny Iran all possible illicit revenue."

- Designating cartels and other related organizations as foreign terrorist organizations (FTOs).

- Lifting sanctions on Syria to strengthen diplomatic ties with new leadership under President Ahmad al-Sharaa.

More broadly, these actions highlight the administration's increased use of the International Emergency Economic Powers Act (the underlying legislation enabling the use of sanctions) to influence foreign policy. For banks and financial institutions worldwide, this evolving landscape necessitates a reevaluation of AML/BSA compliance strategies.

President Trump's second term has ushered in significant shifts in US sanctions policy, impacting financial institutions worldwide.

Operational impact and enforcement expectations

Financial institutions must now contend with an accelerated pace of sanctions-related change and heightened regulatory scrutiny. The Treasury Department, particularly through OFAC, is expected to continue prioritizing enforcement actions aligned with national security interests.

One emerging trend is the administration's push for expanded due diligence responsibilities, such as the proposed imposition of "Know Your Customer's Customer" (KYCC) expectations in certain high-risk areas. In practice, this will challenge existing customer onboarding and transaction monitoring processes, especially for global banks with correspondent relationships.

Furthermore, as sanctions grow more complex and interlinked with trade, export control, and anti-terrorism laws, financial institutions must ensure coordination across compliance, legal, and trade operations teams. Regulators are likely to focus not only on technical compliance but also on governance, escalation procedures, and the ability to implement new sanctions regimes quickly and effectively.

Practical strategies for institutions

To meet the evolving challenge of sanctions compliance in a shifting political landscape, institutions should focus on:

1. **Proactive intelligence monitoring:** Establish internal watchlists and leverage geopolitical intelligence to track sanctions developments. Create escalation pathways to review policy shifts and initiate timely compliance responses.

2. **Enhanced risk assessments:** Refresh enterprise-wide BSA/AML risk assessments with a focus on jurisdictions, industries, and customer types newly impacted by executive actions. Adjust risk scoring models to account for increased exposure to China, Russia, Iran, and entities tied to narcotics trafficking.

3. **Strengthening beneficial ownership and KYC controls:** In anticipation of new regulatory requirements, institutions should revisit their data collection and validation capabilities around beneficial ownership. Enhanced screening and expanded due diligence of customer networks and related parties will be essential.

4. **Screening system optimization:** Tune existing screening platforms to reflect updated sanctions lists and geopolitical risk triggers. Ensure 50% rule compliance by identifying ownership linkages among sanctioned individuals and entities.

5. **Training and culture of escalation:** Bolster compliance training across business lines, with specific case studies and simulations tied to recent executive orders. Encourage a culture of "when in doubt, escalate" to reduce the likelihood of regulatory violations.

How Capco can help

Our financial crime compliance practice helps financial institutions navigate the evolving sanctions landscape with a suite of strategic and execution-oriented services:

- **Sanctions compliance program design and optimization:** We assess current state compliance frameworks against new regulatory expectations and deliver actionable enhancements across governance, policy, and operational processes.
- **KYC and beneficial ownership readiness:** We support banks in implementing customer network screening, ownership threshold assessments, and downstream risk mitigation strategies.
- **Screening technology assessment and tuning:** Our experts fine-tune customer and transaction screening systems, optimize alert quality, and help integrate tools that identify indirect exposure to sanctioned entities.
- **Regulatory intelligence and playbook development:** We deliver horizon-scanning briefs on foreign policy developments and build response playbooks to accelerate implementation of new sanctions programs.
- **Training and awareness campaigns:** We develop and deliver role-specific training to frontline staff, compliance teams, and senior executives on sanctions enforcement risk and best practices.

In today's fast-moving geopolitical climate, banks must be prepared to act swiftly and decisively. Our financial crimes compliance practice combines deep regulatory insight with operational experience to help institutions stay ahead of emerging sanctions risks and maintain regulatory readiness.



26. Navigating PSD3 – a financial crime perspective

The European Commission's proposal for the third Payment Services Directive (PSD3) and the Payment Services Regulation (PSR) represents a pivotal development in the EU's financial regulatory framework. These initiatives aim to modernize payment services, enhance consumer protection, and strengthen the integrity of the financial system. From a financial crime perspective, PSD3 introduces both challenges and opportunities for institutions seeking to bolster their anti-money laundering (AML) and counter-terrorism financing (CTF) measures.

The United Nations Office on Drugs and Crime (UNODC) estimates that money laundering accounts for 2 to 5% of global GDP annually; equivalent to roughly EUR 715 billion to 1.87 trillion each year, highlighting the urgent need for stronger regulations. PSD3 aims to tackle this by improving transparency, strengthening customer identity checks, and making it easier for payment providers and authorities to share information. These changes are designed to close gaps in the system and better protect against financial crime.

Overview and timeline

PSD3, proposed in June 2023, aims to modernize the EU's payment service framework, enhance consumer protection, improve competition, and reinforce the fight against financial crime. It seeks to replace PSD2 by addressing gaps related to fraud prevention, information sharing, and technological advances in payment systems.

The regulation introduces a dual structure:

1. Directive (PSD3) that updates licensing and supervisory frameworks, and

2. Regulation (PSR) that consolidates operational rules for payment services.

While PSD3 will require national transposition, PSR will be directly applicable across the EU. This is likely to become enforceable 18-24 months after adoption, tentatively around 2026.

Immediate action

By the projected 2026 deadline, organizations must:

- **Enhance fraud monitoring systems:** Implement real-time transaction monitoring and AI-driven analytics to detect anomalies and reduce false positives. While this is not strictly mandated under the PSD3 regulation, strengthening fraud detection capabilities aligns with its broader objectives around enhancing consumer protection and trust in digital payments.

- **Upgrade data sharing mechanisms:** Adopt secure and standardized protocols to share fraud-related data across financial institutions.

- **Improve customer authentication:** Strengthen Strong Customer Authentication (SCA) measures in line with updated technical standards.

- **Integrate AML and fraud systems:** Align fincrime strategies with broader enterprise risk management functions.

Preparation should start now with gap assessments, strategy realignment, and roadmap development to ensure compliance readiness.

Industry response and preparations

Organizations across the EU are already mobilizing resources to align with PSD3. Key initiatives include:

- **Investments in technology:** Banks and payment service providers are leveraging machine learning and behavioral biometrics to improve fraud detection and response times. These technologies enable pattern recognition, predictive analytics, and anomaly detection at scale, significantly enhancing the ability to identify and act upon suspicious activities in real time.

- **Collaborative ecosystems:** Institutions are exploring partnerships with fintechs and regtechs to enhance innovation and compliance efficiency.

- **Regulatory engagement:** Active participation in consultations and industry groups is helping firms anticipate final PSD3 provisions.

These efforts reflect a proactive approach, recognizing the strategic importance of PSD3

compliance in maintaining customer trust and regulatory standing.



Key considerations for fincrime teams

Several factors should guide financial crime teams in their PSD3 response:

- **Interoperability of systems:** Ensuring AML, fraud, and cybersecurity systems can communicate effectively is essential for comprehensive threat detection and response. Institutions must prioritize integration platforms and middleware solutions that enable seamless data exchange between disparate systems while maintaining the integrity and confidentiality of sensitive information.
- **Data governance and privacy:** Balancing increased data sharing with GDPR compliance involves robust data classification, access controls, and encryption strategies. Organizations should establish clear data handling policies, perform regular audits, and engage in privacy impact assessments to ensure transparency and accountability.
- **Training and awareness:** Upskilling staff to understand and implement new fraud detection practices requires a structured learning approach. Firms should invest in continuous professional development programs and scenario-based training.
- **Third-party risk management:** Evaluating vendors and partners for compliance readiness and data handling capabilities is critical in minimizing exposure to external risks. This includes conducting rigorous due diligence, setting contractual obligations around data security, and maintaining an ongoing vendor monitoring framework to ensure alignment with regulatory standards.

PSD3 represents a significant shift in the EU payments and financial crime prevention landscape. For firms operating in this space, the directive offers a strategic opportunity to enhance their fincrime frameworks, leverage cutting-edge technologies, and build more resilient financial ecosystems. The time to act is now and with the right guidance, organizations can navigate this transformation effectively and confidently.

How Capco can help

Capco stands ready to support clients through the PSD3 transition with a comprehensive suite of services:

- **Regulatory impact assessments:** Identifying specific requirements and developing tailored compliance strategies.
- **Technology enablement:** We enable smarter alert prioritization and fraud detection through the deployment of advanced analytics, AI-driven models, and intelligence integration tools.
- **Operating model transformation:** Aligning business processes, governance, and organizational structures with PSD3 mandates.
- **Training and change management:** Delivering targeted programs to embed regulatory changes across the enterprise.

With deep industry expertise and a track record of driving regulatory change, Capco empowers institutions to not only meet PSD3 requirements but to turn compliance into a competitive advantage.



Market Regulation

▶ back to contents

27. Transaction reporting: Harmonization and transformation through automation

Introduction

Global regulatory reporting mandatory change remains in sharp focus. The industry is experiencing a clear sense of transition, as impacted firms and regulators navigate the post-implementation effects of significant regulatory rewrites, while also considering the immediate influence of geopolitical developments. Firms face significant short-term challenges with the immediate priority to align with new requirements, repay technical debt, and demonstrate meaningful progress towards the burndown of remediation backlogs. At the same time, there is growing anticipation around how the industry will adopt the expanding capabilities of generative AI (GenAI) as a potential "big bang" solution to the persistent challenges surrounding data quality, supervision, and control in global transaction reporting within the OTC derivatives markets.

Key regulations are still on the horizon. The CSA rewrite is imminent, followed by updates for HKMA, and then continued regulatory change in the US, notably the SEC's Rule 10c-1a on Securities Lending reporting obligations. The prevailing trend continues to be the expansion of data attributes, improved data quality, and the harmonization of reporting standards.



Throughout 2025, firms have been working extensively to ensure compliance with the key regulatory amendments (see Figure 1).

The broader industry seeks to support firms in navigating this pace of change. One such advancement is the International Swaps and Derivatives Association's (ISDA) Digital Regulatory Reporting (DRR) initiative, an open-source, machine-readable and executable solution designed to provide a standardized interpretation of regulatory requirements across multiple jurisdictions. As global regulatory frameworks continue to evolve, shaped by both geopolitical fragmentation and efforts toward harmonization, DRR offers a unified reference point that can help firms manage regulatory divergence more efficiently. It can be implemented either as a core reporting engine or a control layer to validate internal logic, enhancing both transparency and compliance requirements.

The DRR offers a unified reference point that can help firms manage regulatory divergence more efficiently.

The emergence of GenAI further complements tools like DRR, enabling firms to automate data interpretation, accelerate rule mapping, and identify potential gaps in regulatory coverage with greater speed and precision. However, the effectiveness of these innovations still hinges on a firm's ability to ingest, normalize, and represent high-quality transaction data that captures the full complexity of their products, instruments, and business models. In an environment where regulators increasingly demand greater data integrity and explainability, and where geopolitical uncertainty challenges standard-setting efforts, the combination of DRR and AI represents a critical path forward, but only if supported by strong data foundations and robust governance.

Figure 1

2025+

HKMA Rewrite 29th Sept 2025 Go-live

- prioritizes **harmonization** with international standards, introducing **Harmonized UTI (HUTI), UPI, Event Type, and Collateral reporting** — and, unlike CSA, mandates **ISO 20022** for Trade Repository submissions.
- introduces **33 new fields**, aligning technical standards with **IOSCO's Critical Data Elements (CDE)** guidance.
- HKMA will follow **global best practices** established by other recent rewrites.

SEC 10c-1a Jan 2026 Go-Live

- •enhance **transparency in the U.S. securities lending market**, introducing daily position reporting to **FINRA** and guidance on **reporting entity hierarchy**.
- While comparable to **SFTR** in its objectives, 10c-1a reflects a different regulatory approach, underscoring **nuanced differences** across global mandates.
- The rule highlights the challenge of achieving **consistency in interpretation** within a fragmented reporting landscape influenced by regional, regulatory, and institutional differences.
- This complexity is especially critical as **financial penalties for non-compliance** continue to rise, making accurate and aligned reporting more essential than ever.

MiFID 3.0. Q4 2026 Go-Live

- Final report expected by ESMA **June 2025**
- Removal of the **Short Selling Indicator** field from transaction reporting requirements.
- **DLT Identifiers** (DLT IDs) will be added to improve transparency around crypto and digital assets, aligning with MiCA.
- Introduction of fields like **Effective Date, Reporting Timestamp, Waiver Indicator, and OTC Post-Trade Indicator**.
- Adoption of **harmonized reporting timelines** and token identifiers.

Korea October 2025 Go-Live

- Korea's Phase 2 rules begin October 27, 2025, mandating **UPI and CDE reporting** to improve data standardization.
- **OTC derivatives** must be reported to **licensed trade repositories** or firms face fines up to KRW 100 million.
- **Trade repositories** need authorization and must meet governance standards, share data with regulators, and **publish transaction statistics**.
- Firms exceeding **KRW 3 trillion** in **non-cleared derivatives** must post margin under new systemic risk mitigation rules.
- **Cross-border** virtual asset firms must register and **report monthly** to the Bank of Korea from late 2025.

ISO 20022 Q2 2026 Go-Live

- CFTC will adopt ISO 20022 for OTC derivatives reporting, aligning with **global standards** to enhance reporting efficiency.
- ISO 20022 enables **improved interoperability** and more structured, accurate regulatory data for both the SEC and CFTC reporting mandates.
- Firms must update systems and processes to handle ISO 20022 messages, ensuring readiness for 2026 regulatory deadlines and **minimizing compliance risks**.t

CFTC 3.0 Q4 2026 Go-Live

- New data fields proposed for **Parts 43 and 45** to improve surveillance and align with global reporting standards.
- **Geographic masking** will continue post-UPI for certain swaps, with related reporting rule updates also proposed.
- Minor **technical updates** to Parts 43 and 45 clarify data element descriptions and **reporting obligations**.
- Improved **data quality standards** aim to ensure accurate, reliable swap data in line with global expectations.
- Go-live expected late 2026, allowing firms time to **align systems and processes** with new requirements.



What financial services firms should do to prepare

- Prioritize compliance delivery by addressing remediation backlogs, aligning with regulatory RTS, and clearing technical debt across transaction reporting infrastructure.
- Invest in high-quality, structured data that can support expanding reporting fields, new validation rules, and the increased emphasis on data integrity.
- Explore digital regulatory reporting (DRR) as a strategic control layer or core engine to manage regulatory divergence and reduce interpretation risk.
- Adopt GenAI responsibly to enhance rule mapping, exception handling, and impact analysis, with robust controls and explainability in place.
- Strengthen governance and oversight by ensuring robust supervision, reconciliations, and controls that meet growing regulatory expectations.
- Monitor upcoming mandates to stay ahead of jurisdictional timelines and avoid late-stage delivery risks.

How Capco can help

- **Ensure strong data strategy** by assessing data policy, quality, and completeness to support accurate, standardized, and regulator-ready reporting outputs.
- **Apply AI-powered solutions** to map regulations, compare rule changes on a field-by-field basis, interpret cross-regime impacts and assess controls.
- **Conduct an end-to-end system architecture review**, tracing trade data from capture through to regulatory submission, assessing data lineage, control frameworks, and transformation logic at each stage.
- **Streamline requirements capture** using tooling that documents system, policy, and control changes driven by reporting rule rewrites.
- **Deploy experienced teams** that accelerate delivery and support operating model changes across reporting, reference data, and platform architecture.

Conclusion

As the regulatory landscape for **global transaction reporting** continues to evolve at pace, firms must balance compliance with **adaptability**, all while navigating geopolitical uncertainty, emerging technologies, and increasing data scrutiny. Tools like **ISDA's DRR** and the strategic application of **GenAI** offer significant promise, but their success ultimately depends on strong data foundations and thoughtful implementation. **Capco** is ready to support firms through this complex journey, helping them achieve **sustainable compliance** by aligning regulatory requirements with scalable, efficient, and future-proof reporting solutions.



> **As the regulatory landscape for global transaction reporting continues to evolve at pace, firms must balance compliance with adaptability, all while navigating geopolitical uncertainty, emerging technologies, and increasing data scrutiny.**
>
> **Marija Devic**
> Executive Director

back to contents

28. Impact of deregulation in the US

The impact of deregulation in the US has been uneven since President Trump took office. While the financial services industry has welcomed deregulation, the process with which it is taking shape does not give financial institutions a clear understanding of what specific areas within laws or regulations will be prioritized. This lack of an articulated framework from which the industry should respond is causing financial institutions to respond in nearly real-time to actions taken by the Trump administration.

The whipsaw of policy effects does not give financial institutions a clear policy framework for which areas to prioritize or deprioritize.

The Trump administration has a number of tools to reduce or eliminate regulatory burdens, including proposing or rewriting rules under the Administrative Procedure Act (APA), disapproving of final regulations under the Biden administration through the Congressional Review Act (CRA), deprioritizing enforcement of specific rules, withdrawing from litigation, and any number of administrative tools that can affect public policy and supervision. Since President Trump's first hundred days in office, he relied upon two main policy and administrative tools to impact regulation by issuing Executive Orders (EOs) and significantly changing the staffing levels at the various government agencies.

The broad use of these tools has caused financial institutions to monitor not only for guidance or policy changes directly from the agencies but also for litigation in the federal courts that instantly reverses actions taken by the administration. This whipsaw of policy effects does not give financial institutions a clear policy framework for which areas to prioritize or deprioritize, make changes to policies and procedures, or focus resources. Currently, deregulation is becoming as burdensome as regulation. The expectation is that the impact from the current deregulatory approach will be stabilized as the heads of the various agencies are confirmed by the US Senate and can focus on long-term policy changes that can be structured into the rulemaking process.

In addition to federal deregulation efforts, the states are focused on two areas: slowing or mitigating efforts by the Trump administration to affect financial services policy. The first is through litigation in both state and federal courts to stop, reverse, or otherwise prevent the Trump administration from reducing staffing levels, closing agencies, firing independent agency leaders, and changing enforcement of laws and regulations. Over two hundred lawsuits are, in various stages, making their way through the courts, and more are expected to be filed as the President moves forward with his priorities.

The second effort by the states is on changes to financial services state laws and regulations that can replace federal policy changes. Financial institutions





must monitor for policy changes at the federal level and respond to actions taken to pass new laws and regulations where they operate. States have passed legislation on artificial intelligence (AI), climate change, junk fees, overdraft, and community reinvestment. These changes to state law have been further supported by various states taking a more aggressive approach to financial services regulation and enforcement. Examples of these efforts include actions to eliminate the reporting of medical debt on consumer credit reports, provide consumer protections for AI, and enforce cryptocurrency laws and regulations.

Over two hundred lawsuits are, in various stages, making their way through the courts, and more are expected to be filed as the President moves forward with his priorities.

While financial services welcome the idea of deregulation, they have not welcomed the challenges of tracking and responding to nearly real-time policy, regulatory, and operational changes at the federal level, coupled with litigation and changes to laws, regulations, and enforcement at the state level. Financial institutions are encouraged to continue to focus on complying with current, applicable federal and state laws and regulations and maintaining comprehensive compliance and risk management programs.

It is further suggested that financial institutions fine-tune their regulatory surveillance program to monitor changes from state banking and securities regulators, state attorneys general, the office of the governor, and litigation reported by state and national trade associations. Pending new developments and additional clarity in the evolving regulatory landscape, we encourage our clients to continue business as usual, particularly when managing, administering, and optimizing their compliance and risk management programs.

How Capco can help

Geopolitical risk management is becoming increasingly an operational imperative. Capco can help financial institutions not only manage the risks from non-compliance due to conflicting internation, federal, and state laws, but also become proactive in taking advantage of emerging trends in predictive risk management. Financial institutions must pivot from responding to geopolitical risk on a short-term ad-hoc basis with a narrow lens, and instead develop a centralized strategy and single risk management approach that focuses on servicing the entire geopolitical landscape that provides key data points and analysis that integrate into a firm's overall operational risk management strategy.

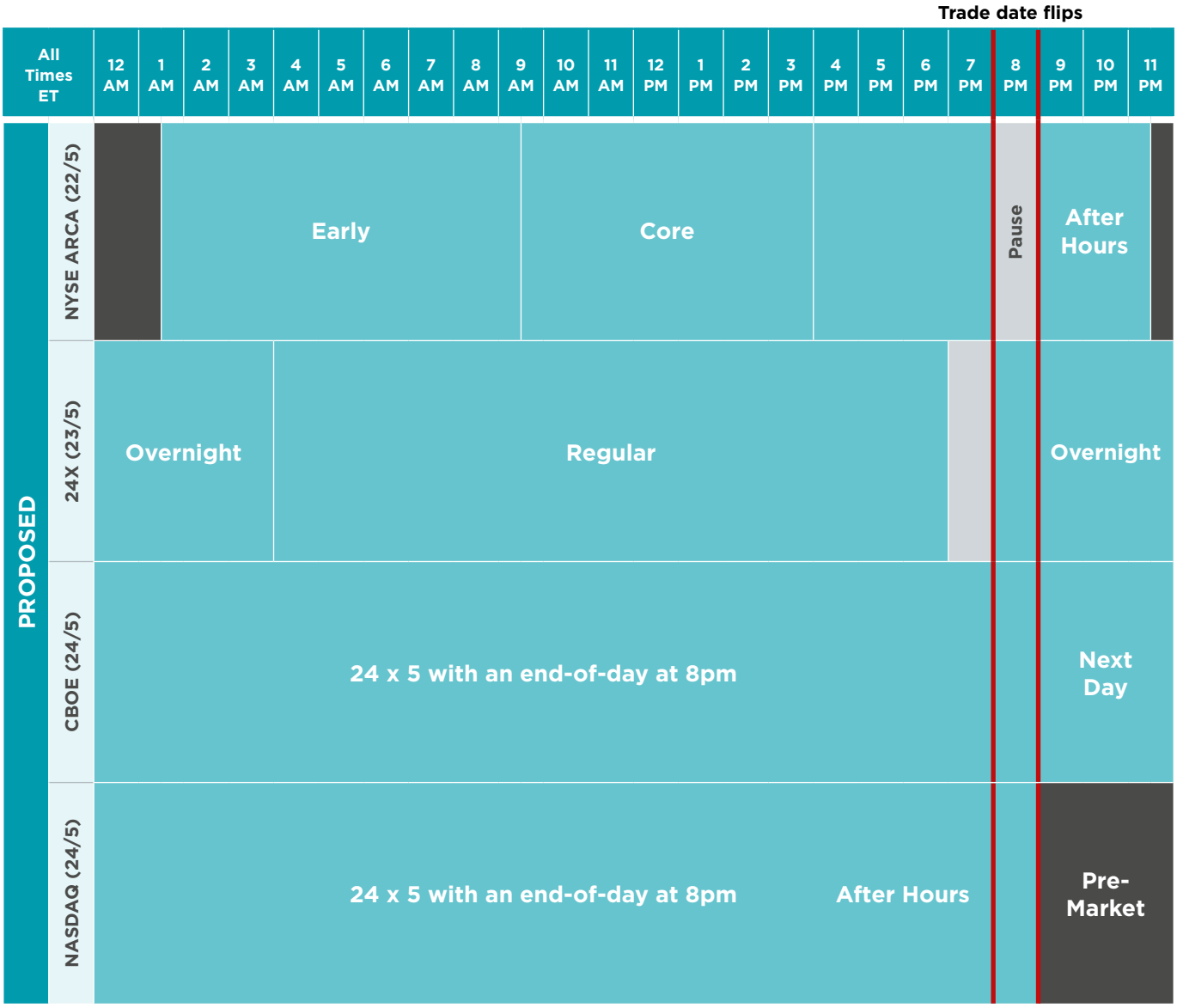
Capco has utilized its extensive experience and subject matter expertise to develop a flexible regulatory program delivery methodology to proactively tackle geopolitical risks in a holistic way.

29. US extended trading hours: Impact assessment for investors and broker-dealers

"Beyond the closing bell," "after-hours," and/or "extended hours" trading capabilities have been highlighted by digital retail brokerage firms as key levers to enable individual investors globally to continue interacting with the market, react to late-breaking news, and capitalize on price shifts.

A few headline developments in the US highlight an acceleration in this march towards extended trading hours: between October 2024 and March 2025, NYSE ARCA, 24X, CBOE and Nasdaq have either submitted proposals to the SEC to operate in an overnight trading capacity or announced plans to do so.

Fig. 1. Extended trading sessions: Market landscape



Legend Key

Market Closed | Pre-Market Trading | Trading Hours

Sources: Publicly available announcements from listed companies & current industry conjecture as of April 2025



While intriguing and potentially promising, such extended windows into non-standard hours for trading can give rise to challenges, complexities, and risks.

Impacts on institutional investors

Market dynamics: The extended hours could enhance price discovery, particularly around major announcements or economic data releases that occur outside standard trading hours.

Increased flexibility: Global investors in different time zones will have more opportunities to trade US equities and ETFs.

Liquidity and volatility: While extended hours can increase overall market liquidity, they often mean higher volatility and wider bid-ask spreads due to lower off-peak trading volumes.

Operational adjustments: Institutional investors might need to adapt their strategies and operations (e.g., with location strategy optimization), to take advantage of the extended trading window.

Technology and costs: Investors may need advanced trading tools to navigate the extended hours effectively, which could increase costs for those without industry-leading capabilities and resources.

Impacts on broker-dealers

Operations and technology adjustments

- **Corporate actions:** Deadlines for participation in voluntary events may be driven right up to agent deadlines, leaving no time for the largely manual process of reconciling and processing instructions. Resulting securities may be tradeable immediately leaving no room for any processing errors.

- **Staffing:** Broker-dealers will need to implement multiple shifts or hire additional staff to ensure continuous coverage, including client services and support.

- **Technology upgrades:** Enhanced trading systems and infrastructure will be necessary to support the added trading activity. This includes upgrading servers, improving network capabilities, and implementing robust cybersecurity measures.

Risk management.

- **Order execution risk:** Low trading volumes in extended hours can result in partial fills or unfavorable pricing, though they could be mitigated with limit order preference, which provides more price control.

Between October 2024 and March 2025, NYSE ARCA, 24X, CBOE and Nasdaq have either submitted proposals to the SEC to operate in an overnight trading capacity or announced plans to do so.

- **Increased volatility:** Extended trading hours often come with higher volatility, as trading volumes are lower during off-peak times. Broker-dealers will need to enhance their risk management systems and personnel to monitor and respond to rapid price movements outside of traditional business hours.

- **Liquidity management:** Managing liquidity will be more challenging during extended hours due to lower trading volumes. Broker-dealers will need to ensure they have sufficient liquidity to meet trading demands and avoid significant price impacts from wider spreads.



- **Operational resilience:** Broker-dealers will need to ensure their systems and processes are resilient to handle the increased operational demands.

Regulatory compliance

- **Continuous monitoring and reporting:** Broker dealers will need to ensure continuous monitoring and reporting of trading activities.

- **Enhanced surveillance:** Regulators may require enhanced surveillance measures to detect and prevent market manipulation and other illicit activities during extended hours. This includes using GenAI, advanced analytics and machine learning tools to identify unusual trading patterns.

- **Adherence to market and regulatory rules:** Extended trading hours mean broker-dealers must comply with market rules and regulations around the clock. This includes potential registration requirements for overseas office branches and personnel.

Cost management

The need for continuous operations could lead to higher costs (e.g., staffing, technology, infrastructure) to ensure seamless trading during extended hours. Impacted firms will need to innovate, optimize, or automate processes if they want to maintain their current operating costs.

Conclusion

On balance, the expansion of extended hours trading capabilities seems to be an inevitable forward-looking evolution, promising greater flexibility and accessibility for domestic and global participants in the US equity markets. However, it does present risks as well as opportunities for investors, as well as for broker-dealers, who need to weigh the pros and cons of this shift in the context of their trading strategies.

At Capco, we help buy-side and sell-side firms embrace the opportunity of extended trading hours. We transform organizations based on our capital markets expertise and can help financial institutions address the impacts and challenges related to this initiative.



> **The need for continuous operations could lead to higher costs (e.g., staffing, technology, infrastructure) to ensure seamless trading during extended hours. Impacted firms will need to innovate, optimize, or automate processes if they want to maintain their current operating costs.**
>
> **Thanh Le Xuan**
> Managing Principal

▶ back to contents

30. Market-wide Half-Hourly Settlement Programme (MHHS)

The Market-wide Half Hourly Settlement (MHHS) Programme marks a seismic shift in the UK electricity market since deregulation in the 1990s. It moves the measurement and billing of electricity to a half hourly billing and settlement cycle and replaces outdated settlement systems. This is a key enabler of the flexibility to support the transition to Net Zero and decarbonization. MHHS is one of Ofgem's five leading strategic priorities. The program will contribute to a more effective electricity system, encouraging more flexible use of energy and helping consumers reduce their bills.



Objectives of the regulatory change

The change to half-hourly settlement brings more flexibility to the energy system and allows better integration of renewable energy sources and other flexible technologies. It also facilitates the more intelligent patterns of consumption such as time-of-use tariffs.

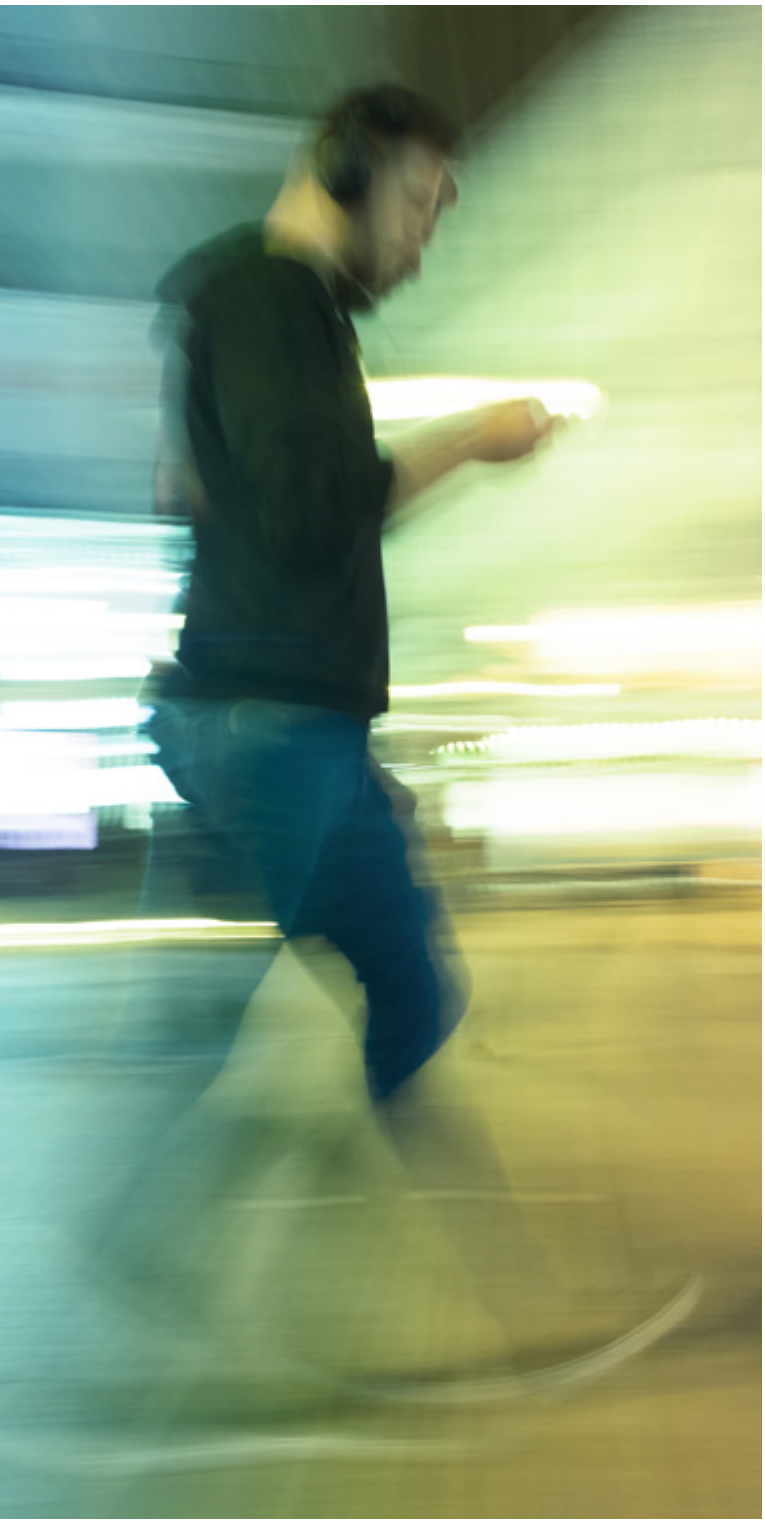
The new half-hourly settlement process enables suppliers ultimately to match up trading, expected customer demand, and actual usage. The program aims for all electricity market trading in the UK to be based on accurate half-hourly data by October 2026.

An advantage of MHHS is that consumers will be incentivized to move their consumption away from peak periods by using technologies, such as battery storage and electric vehicles, to grid functionality. This change in consumption patterns will help avoid expensive network reinforcement works and also facilitate the use of renewables as demand is smoothed out.

Implementing MHHS presents several data and technology challenges. The key challenges are described below:

- **Data collection and management (volume and frequency):** The transition to half-hourly data significantly increases the volume of data being collected across millions of customers, with data captured every 30 minutes instead of once a year

- **Data standardization:** Ensuring all data is standardized across the market to ensure consistency, accuracy, and compatibility across the system



- **Data integrity:** Ensuring the reliability and accuracy of data, especially when gathering it from multiple sources (e.g., smart meters, grid systems, and third-party providers)

- **Legacy systems:** Integrating new half-hourly data streams with existing legacy systems, which were built for annual or monthly data processing is a major challenge

- **System interoperability:** Ensuring smooth data flow and communication between different market participants, such as suppliers, distribution network operators (DNOs), and settlement bodies

- **Data privacy:** Given the sensitive nature of electricity usage data, ensuring robust security measures are in place to protect customer privacy and meet GDPR compliance requirements

- **Regulatory requirements:** Adhering to stringent Elexon and Ofgem rules while ensuring timely and accurate data reporting

- **Real-time data processing:** The half-hourly data needs to be processed and analyzed quickly for settlement and forecasting. Companies need the infrastructure to handle high-frequency data and provide timely insights.

MHHS is a key enabler of the flexibility to support the transition to Net Zero and decarbonization.

- **Advanced analytics:** Using data analytics to predict consumption patterns, detect anomalies, and optimize energy pricing can be challenging with the volume and complexity of data

- **Billing complexity:** Transitioning to half-hourly data requires new billing systems capable of processing large volumes of granular data, which impacts customer communication, invoicing, and dispute resolution.

The following strategic considerations have been identified by Capco to address the key technological challenges:

- **Build scalable data platforms:** Develop a flexible and scalable cloud platform capable of handling high-frequency data collection and processing at scale.

- **Data lake and integration hub:** Establish a data lake to consolidate half-hourly consumption data,



and an integration hub to connect all market participants (DNOs, suppliers, regulators) for seamless data flow.

- **Implement real-time data processing systems:** Develop data pipelines to efficiently handle the ingestion, cleaning, and processing of large volumes of half-hourly data in real-time.

The program aims for all electricity market trading in the UK to be based on accurate half-hourly data by October 2026.

- **APIs for interoperability:** Develop standardized APIs to enable smooth data exchange and interoperability between suppliers, DNOs, and regulators in the market.
- **Enhance data analytics and forecasting capabilities:** Build advanced predictive analytics tools to forecast demand, consumption patterns, and pricing trends based on half-hourly data.
- **Machine learning models:** Implement machine learning algorithms for anomaly detection, energy demand forecasting, and optimizing the settlement process to improve pricing accuracy and efficiency.
- **Demand response optimization:** Use analytics to create dynamic pricing models and identify opportunities for demand-side flexibility to balance grid load.
- **GDPR and security frameworks:** Implement strong cybersecurity to secure sensitive customer data and ensure full compliance with GDPR and Ofgem regulations.
- **Compliance automation:** Develop automated tools to ensure that data collection, reporting, and settlement processes adhere to all regulatory requirements, reducing the risk of non-compliance penalties.
- **Customer engagement platforms:** Build customer portals that allow consumers to view their half-hourly data, access detailed billing information, and receive insights into consumption patterns and energy savings.

Conclusion

Successfully implementing MHHS requires addressing significant data and technology challenges. Capco is in a strong position to support market participants through its industry award winning data practice servicing the energy and financial services sector.

31. Energy Retail Market Reform – Phase 2



Energy Retail Market Reform – Phase 2 is a series of regulatory initiatives introduced by Ofgem, the UK's energy regulator, aimed at improving the functioning of the energy retail market. This phase builds on earlier reforms and focuses on enhancing the market's efficiency, fairness, and resilience. Below is an overview of the key elements of Phase 2 of the Energy Retail Market Reform:

- **Faster switching:** the introduction of faster switching mechanisms, reducing the time it takes for customers to change energy suppliers. The aim is to empower consumers to switch suppliers more easily, leading to more competitive pricing and better service offerings.

- **Prepayment meters:** focused on improving protections and options for consumers with prepayment meters, providing better support for vulnerable consumers, and ensuring they have access to competitive tariffs.

- **Smart meter rollout:** aiming for a nationwide infrastructure where customers can better manage their energy consumption. This allows for more accurate billing, clearer insight into energy usage, and potential cost savings.

- **Protection for vulnerable consumers:** enhancements to current rules to protect vulnerable consumers by introducing targeted measures. These may include improving support for those in financial distress, better access to payment plans, and ensuring vulnerable customers are not left behind as the market transitions.

- **Increased transparency and information:** the need for better, clearer communication from energy suppliers to consumers, helping them make more informed decisions. This includes clearer tariff structures, better information on billing, and more accessible advice for consumers.

Phase 2 of the reforms is expected to unfold over a series of years. Key elements, such as faster switching and smart meter expansion, are already being implemented, while others will require coordination between Ofgem, energy suppliers, and consumer advocacy groups.

The following are key data and technology challenges identified for Phase 2 implementation:

- **Fragmented and legacy data systems:** Many suppliers operate on outdated legacy systems not designed to support real-time switching, smart metering integration, or dynamic tariff models. Furthermore, disconnected data systems create operational inefficiencies.

- **Lack of automation and interoperability:** Faster switching requires near-instantaneous data validation and communication across market participants. Current systems often lack the automation and interoperability to support this. Prepayment and smart meter data need to be processed in near real-time for accurate billing and customer engagement.

- **Data accuracy and customer trust:** Inaccurate or incomplete customer data undermines transparency, disrupts switching, and leads to billing errors, especially critical when dealing with vulnerable customers. Maintaining up-to-date and verified customer profiles is a growing challenge.

- **Cybersecurity and data privacy:** Smart meter rollouts and centralized data models expand the attack surface for cyber threats. Ensuring GDPR compliance while sharing data across systems adds complexity.

- **Consumer-facing digital experience:** Regulatory demand for clearer tariffs, billing transparency, and digital support tools requires energy suppliers to transform the customer interface with more dynamic and personalized digital services.

The Energy Retail Market Reform – Phase 2 is not just a regulatory update, it is a data transformation mandate.

Capco can help the energy industry to ensure compliance with upcoming regulations through the following:

- **Support for vulnerable customers:** translating our expertise from management of associated regulatory risks in financial services to help deliver good outcomes for customers. This includes helping to assess current controls and processes for identifying and managing vulnerable customers and helping create management KPIs to evidence for internal and external stakeholders how the firm actively manages and supports vulnerable customers.

- **Digital architecture modernization:** Assess and re-architect existing systems to support modular, API-enabled platforms that can handle high-frequency, real-time data flows. Design enterprise data platforms that unify data across CRM, billing, metering, and regulatory reporting systems.

- **Data quality and governance frameworks:** Implement data cleansing and enrichment solutions to create single customer views that enable accurate billing, vulnerability identification, and switching eligibility. Establish robust data governance frameworks to ensure compliance, traceability, and accountability for consumer data.

- **Smart meter data integration:** Build integration layers and analytical models to ingest and operationalize smart meter data for dynamic pricing, real-time usage insights, and demand-side management. Use data analytics to detect anomalies, track usage patterns, and personalize customer engagement strategies.

- **Secure, compliant data sharing:** Develop secure data exchange mechanisms (e.g.. encrypted APIs) that support faster switching and cross-party coordination while meeting GDPR and Ofgem standards. Deploy automated consent management tools to ensure ethical and compliant use of personal data.

- **Customer experience and digital tools:** Design and deploy user-centric digital platforms that improve communication, simplify tariff comparison, and provide actionable usage insights for customers. Introduce AI-powered chatbots or virtual agents to support vulnerable customers with tailored advice, payment options, and service accessibility.

Conclusion

The Energy Retail Market Reform – Phase 2 is not just a regulatory update, it is a data transformation mandate. Suppliers must evolve their control frameworks, systems, processes, KRIs, and digital channels to align with Ofgem's push for competition, transparency, and customer protection.

How Capco can help

Capco is uniquely positioned to guide this transformation by blending deep sector knowledge with data engineering, regulatory expertise, and digital innovation. By addressing data fragmentation, enabling real-time processing, and implementing effective controls to identify, assess and evidence support for vulnerable customers, Capco can help energy suppliers build a future-proof, consumer-centric, and compliant retail energy ecosystem.



“

Capco can help the energy industry to ensure compliance with upcoming regulations and support vulnerable customers, translating our expertise from management of associated regulatory risks in financial services to help deliver good outcomes for customers.

Saeed Patel
Executive Director

▶ back to contents

32. UK T+1 Settlement: Time enough for implementation, but still no time to waste



The UK Accelerated Settlement Taskforce (AST) has published its final T+1 implementation plan marking a critical step towards a faster and more efficient securities settlement process. This move aligns the UK with a global trend toward faster settlement times aiming to reduce counterparty risk, enhance market efficiency, and improve liquidity.

At her February 19th meeting with the investment banking and asset management sectors to refine the government's Financial Services Growth and Competitiveness Strategy, Chancellor of the Exchequer Rachel Reeves reaffirmed the importance of going further and faster to drive growth and revealed that the government had accepted all recommendations made by the Accelerated Settlement Technical Group. "Speeding up the settlement of trades makes our financial markets more efficient and internationally competitive," she said.

At the same meeting, FCA CEO Nikhil Rathi confirmed that the regulator "expects firms to engage and plan early." Andrew Bailey, Governor of the Bank of England, added: "It is important that firms and settlement infrastructures have robust plans for an orderly transition in October 2027. As part of this effort, the Bank looks forward to continuing dialogue with regulators in other markets which are pursuing similar changes."[31]

The AST's implementation plan includes a Code of Conduct that highlights 12 critical operational actions and 26 recommended actions to ensure a smooth transition. The AST also advises that all major changes should be completed by the close of 2026 to facilitate this transition.

While firms know this change is coming, many are not entirely clear about what they should be doing now. Below we look to address these questions in a sensible and pragmatic way.

Mark your calendar

October 11, 2027 is the day UK cash securities trading will officially move to T+1, but – per the AST's advice

31. https://www.gov.uk/government/news/chancellor-goes-further-and-faster-to-drive-growth-by-speeding-up-securities-trades

– firms should be fully tested and ready well before this date.

To increase settlement rates, firms may require significant operational and technological upgrades, particularly in respect of trade matching, reconciliations, and post-trade automation. With tighter timeframes to manage exceptions, market participants, including investment banks, asset managers, and custodians, must invest in minimizing time-consuming manual exception processes to avoid settlement failures.

Additionally, the compressed settlement window may increase funding and liquidity pressures, particularly for international investors who rely on foreign exchange, which have historically worked to T+2 cycles, and securities lending recall processes that will now need to operate to shorter timelines.

Andrew Douglas, chair of the AST, has urged market participants to start planning now, mobilize their initiatives, and secure appropriate budget allocations for project funding through 2026. He has emphasized that "automation will be a key component of a successful implementation," helping firms to manage the accelerated timeline effectively.[32]

The plan provides more detail on the required automation, particularly in respect of the AST's five "expected behaviors" – commitment to compliance, automation, "action this day," settlement discipline, and readiness for testing – which should be helpful to the industry in planning and driving readiness efforts.

We would note the following highlights from the AST plan:

- The encouragement to compliance and internal audit functions, as well as by extension regulators, that they reference the Code of Conduct when assessing performance – line teams need to be ready to explain how they are aligning to the Code.

- The reiteration that the industry needs to be ready for market testing by the start of 2027 – so all major changes should be complete and in place by the end of 2026.

- The specific call out for automation of Standard Settlement Instruction (SSI) processing, corporate action processing, and stock lending recalls – these all are actionable priorities that the industry should take seriously and engage with now.

To address these priorities, participants should look to build and/or utilize stock ladders in real-time to ensure inventory is in the correct place or has been recalled from loan to enable timely settlement. They should ensure they continuously improve their settlement performance through correctly identifying fail reasons and working on fixes for repeated pre-matching or settlement issues.

The industry needs to be ready for market testing by the start of 2027 – so all major changes should be complete and in place by the end of 2026.

The securities post-trade space is a focus for a number of interesting and potentially useful technology and operational service vendors and innovative market infrastructure initiatives. As it can take time to onboard these and incorporate them into operational processes, firms should assess these options during 2025 to determine whether any might be a useful part of their approach.

And finally, to get benefit from these investments, over and above alignment with the new market standard, firms should ensure that the data lens through which they assess settlement performance is not confined to settlement performance in terms of numbers of trades, but also takes in transaction value and risk.

So, while there is sufficient time to plan and execute a high-quality T+1 initiative for the UK and Europe, aligning to the market convention and realizing benefits, there is no time to waste.

32. https://acceleratedsettlement.co.uk/publishes-final-implementation-plan/



Financial Risk

▶ back to contents

33. Reviewing the ECB Pillar 2 Requirements methodology

Overview

In March 2025, the European Central Bank (ECB) announced a review of its Pillar 2 Requirements (P2R) methodology. This is in line with its **broader review** of the Supervisory Review and Evaluation Process (SREP) to make European banking supervision more efficient and effective.

The new approach aims to simplify (see Appendix) and strengthen the connection between capital requirements and banks' underlying risk profiles as assessed through the SREP. However, the ECB will maintain its practice of using SREP decisions to convey Pillar 2 requirements, along with clear insights into the key risk drivers influencing those decisions.

One of the key changes is the ECB's focus on evaluating individual risk areas separately (i.e., risk-by-risk capital charges), allowing for a more granular and tailored capital requirement. Additionally, banks with prolonged weak internal controls and governance are likely to receive higher capital requirements due to these shortcomings. While banks may not yet be able to fully gauge the impact of the new methodology on their overall capital requirements, the ECB has stated that it does not expect any abrupt changes.



Whilst the implementation phases are staggered, banks that act now will be better positioned to absorb shocks, meet supervisory expectations, and make capital allocation a more strategic function.

Although the ECB mentions that the Internal Capital Adequacy Assessment Process (ICAAP) will no longer directly determine P2R, we believe that banks should continue to leverage ICAAP as a strategic tool for capital planning and defining risk appetite.

Next steps

The ECB intends to pilot this new approach internally in 2025, with full implementation from the 2026 SREP cycle, and updated P2Rs coming into effect on January 1, 2027. Whilst the implementation phases are staggered, banks that act now will be better positioned to absorb shocks, meet supervisory expectations, and make capital allocation a more strategic function.

Conclusion

This shift presents both opportunities and challenges for banks, necessitating stronger analytical capabilities, upgraded risk and data infrastructure, and more proactive, transparent engagement with supervisors. Additionally, this serves as a call to action and an opportunity for banks to assess their own risk appetite and act accordingly.

Below are key areas of consideration for banks:

Topic	ECB's reference	Potential implications and proposed approach
Risk-based SREP scoring	"In the revised methodology, Pillar 2 requirements will be driven more directly by relevant areas of risk, and higher risks will continue to result in worse SREP scores and a higher Pillar 2 requirement."	**Potential implications:** Banks without a well-defined, proactive strategy to manage material exposures in "higher risk" areas will be among the most impacted by the revised Pillar 2 framework. **Proposed approach:** To support effective risk management, banks should proactively classify risks according to their materiality and potential impact. For instance, universal banks with high exposure to leveraged lending or commercial real estate portfolios may see increased capital charges unless robust risk mitigation strategies are in place.
Supervisory discretion applied	"The new Pillar 2 requirement methodology will allow supervisors to exercise judgement as they score individual risk elements, apply the risk-by-risk approach to determine capital requirements for each relevant risk area individually."	**Potential implications:** Banks with weak internal risk identification and analysis processes will be more exposed to supervisory judgement. **Proposed approach:** Banks should regularly update risk taxonomies and ensure that exposures such as climate-related financial risks, IT/cyber risks, or new product risks are explicitly assessed in alignment with new enforced regulation (DORA, CRR3, CSRD, and EBA Guidelines on ESG Risk).
Total risk profile	"Assess a bank's overall risk profile, which might be more complex than the sum of its individual parts."	**Potential implications:** Banks that maintain a fragmented view of risk are more likely to underestimate their overall risk exposure, increasing the chance of unexpected losses. In recent cycles, banks with inconsistent risk views, for example, those underestimating IRRBB impact under rate shocks, have faced increased P2R components despite having adequate Pillar 1 metrics. **Proposed approach:** Conduct forward-looking reviews that not only assess individual risk exposures such as credit, market, and liquidity risk, but also consider how these risks interact with one another under adverse stress scenarios.
Internal controls and governance oversight	Pillar 2 capital requirements can be influenced more directly if internal controls weaknesses or governance issues are not resolved promptly and if other supervisory measures prove to be insufficient.	**Potential implications:** Banks in this position may face increased Pillar 2 capital requirements, along with heightened supervisory scrutiny and potential reputational risks. **Proposed approach:** Banks should ensure regular and documented involvement of the board in risk governance, maintain independent model validation functions, and ensure that audit findings are remediated on time with clear escalation procedures.

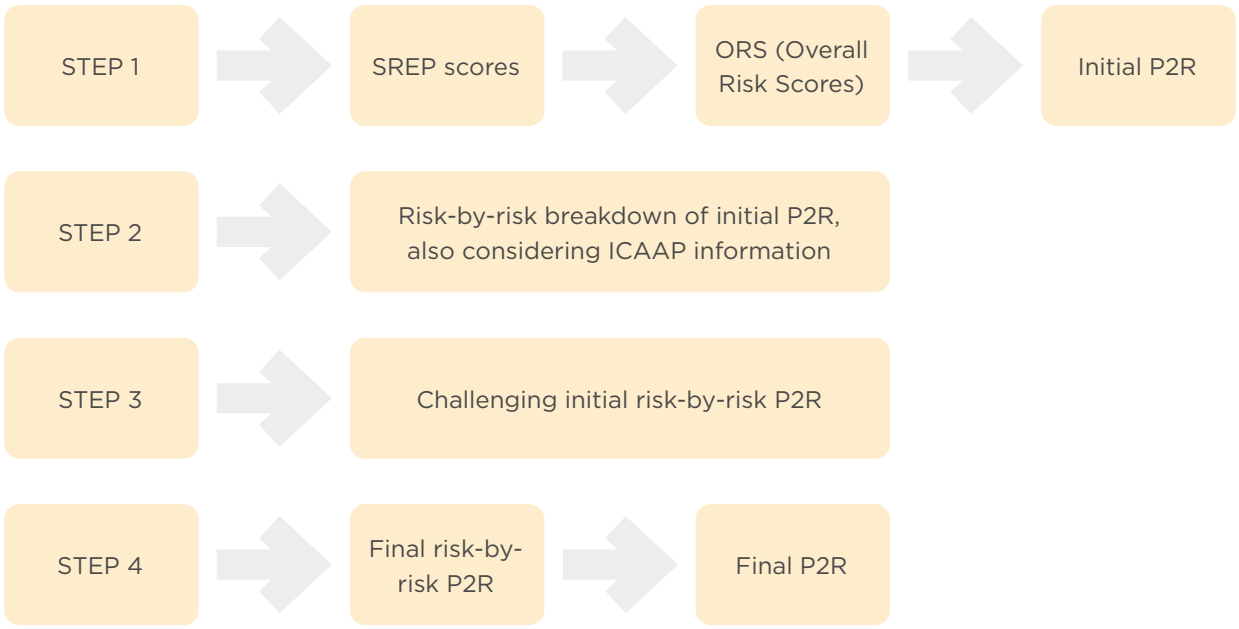
How CAPCO can help you navigate the ECB's Pillar 2 Capital Requirement



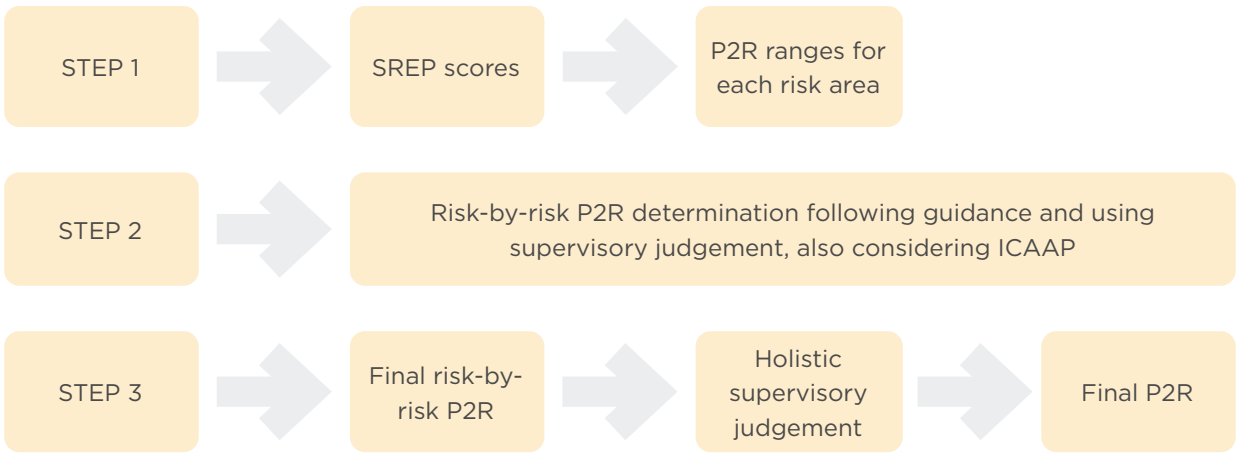
ICAAP Diagnostics and Enhancement	• End-to-end review and documentation of ICAAP, process flows, and governance structures. • Support with embedding ICAAP into strategic planning, risk appetite and capital allocation processes • Support with the alignment of ICAAP with Recovery Plan. • Review and enhance Risk Management Framework and Policies.
Data & Model Management	• Strengthening of data lineage, model governance, and internal model documentation. • Alignment of risk data aggregation capabilities to supervisory and internal needs.
Scenario design and stress testing transformation	• Conduct gap assessment of stress testing framework against ECB supervisory expectations and leading industry practices. • Design and implementation of enhanced stress testing frameworks aligned to regulatory expectations. • Integration of climate, geopolitical, and macroeconomic risk scenarios. • Testing of effectiveness of controls over scenario design and stress testing processes.
AI & Predictive Analytics	• Leveraging AI to improve scenario design, early warning systems, and capital planning. • Use of machine learning to detect anomalies and streamline risk monitoring.

Appendix

Current P2R* Methodology



Revised P2R* Methodology



***P2R stands for "Pillar 2 Requirement"**

Source: Reviewing the Pillar 2 requirement methodology

34. OSFI outlook: Credit and liquidity risk

In our overview of the Canadian regulatory landscape, we covered OSFI's 2025-2026 Annual Risk Outlook, which lists "Wholesale Credit Risks" and "Funding and Liquidity Risks" as among the top threats to Canada's financial system. This was alongside related concerns to mortgage and real estate secured lending (RESL) risk on the consumer side.

Canadian commercial businesses are facing a perfect storm: interest rates remain above historical trends despite recent relief, resulting in elevated debt servicing costs. This is compounded by broader macroeconomic uncertainty, including a dynamic political situation and rising trade protectionism. While commercial loan delinquencies have not yet triggered significant credit losses, OSFI notes an upward trend from historically low levels.

As recent global bank failures have shown, stress can propagate rapidly through highly digitalized banking systems.



On the liquidity front, OSFI states that the funding environment is currently stable. General market confidence has supported steady deposits and continued access to wholesale funding. However, the regulator also highlights geopolitical uncertainties and an elevated risk of shocks. These are driven by sudden market shifts, volatile trading environments, increased incorporation of volatile assets like crypto in the global financial systems, and the threat of international trade wars involving the US, China, and Europe. Liquidity shocks could materialize quickly. As recent global bank failures have shown, stress can propagate rapidly through highly digitalized banking systems, especially with Canada's expected launch of real-time payments and digital banking now the norm. Although Canada has so far avoided these crises seen in the US market, its concentrated and highly interconnected banking sector introduces structural vulnerabilities, elevated by CDIC's lower deposit insurance coverage levels.

Residential mortgage and real estate secured lending (RESL) risks continue to be a concern. Despite the recent decline in interest rates, a significant wave of mortgage renewals and refinancing is expected over the next two years. As of late 2024, 36% of outstanding mortgages were due for renewal by the end of 2026, many of which were originated during a period of ultra-low rates. Combined with cost-of-living increases, many Canadian households, particularly in highly leveraged markets such as Toronto and Vancouver, are expected to face substantial affordability stress upon renewal.

OSFI's regulatory response

In response, OSFI will intensify its scrutiny around these risks. Banks should expect increased data requests, including a new loan-level, non-retail data call focused on wholesale credit exposures. This is part of a broader effort to assess banks' credit risk management practices, including underwriting

standards, account management, internal risk ratings, and preparedness for a potential downturn.

On the liquidity side, OSFI will test institutions' resilience to complex stress scenarios. This includes examining the robustness of liquidity limits, contingency funding plans, and risk appetite statements. OSFI will also open consultations on updates to its Liquidity Adequacy Requirements (LAR) guideline and will introduce a more structured Internal Liquidity Adequacy Assessment Process (ILAAP). This will require each bank to develop holistic liquidity plans and conduct internal stress tests designed to evaluate resilience to severe liquidity pressures.

A call to action for financial institutions and regulators

Navigating these dynamic times will require more than institutional resilience, it will demand support for customer resilience as well. Banks must shift from a purely defensive risk posture to a proactive customer engagement strategy if they are to avoid major pitfalls in the years ahead. Inflation remains stubborn, protectionist policies are introducing friction into trade, and interest rates cannot be relied upon to return to pandemic era lows.



Key actions for banks include:

- **Support financial wellness**
  With mortgage renewals looming and household budgets under strain, banks should take the lead in identifying vulnerable borrowers early. Personalized outreach, refinancing options, and proactive engagement can prevent defaults before they occur, protecting customers and balance sheets.

Banks must shift from a purely defensive risk posture to a proactive customer engagement strategy if they are to avoid major pitfalls in the years ahead.

- **Elevate SME engagement**
  Credit risks are rising not only for large corporates, but also for small- and medium-sized enterprises (SMEs). Banks must treat SME credit with the same strategic importance as retail lending, recognizing that cash flow volatility, inflation pressure, and refinancing risks mirror those in the household sector. Holistic relationship management and flexible financing solutions will be essential.

- **Embed resilience across the enterprise**
  From rigorous stress testing to liquidity contingency planning, risk leaders must ensure that their institutions are prepared for sudden shocks, whether from markets, geopolitics, or domestic downturns. Waiting for a crisis to act is no longer prudent.

- **Modernize liquidity risk practices**
  OSFI's expectations for 2025-2026 are clear: simulate complex, multi-jurisdictional liquidity scenarios that reflect current funding risks, including reliance on wholesale markets, cross-border challenges, and foreign exchange mismatches. Internal systems must also support dynamic, real-time intraday liquidity monitoring. In an era of digital banking and instant payments, liquidity stress can unfold in hours.

35. Dynamic General Insurance Stress Test (DyGIST)

Background

In December 2024, the Prudential Regulation Authority (PRA) announced the deferral of the first Dynamic General Insurance Stress Test (DyGIST) to May 2026. This adjustment was made in response to the upcoming implementation of the Solvency UK reforms, which are expected to place significant demands on insurers' resources. The deferral is intended to reduce the operational strain that would have resulted from running both the Life Insurance Stress Test (LIST 2025) and the new DyGIST in the same calendar year.

Under the revised schedule, the PRA will now conduct life insurance stress tests biennially starting in 2025, and general insurance stress tests biennially from 2026, allowing firms to allocate resources more effectively and focus on the evolving regulatory landscape.

However, this should not be interpreted as a pause in regulatory scrutiny, but rather as a recalibration towards a more pragmatic timeline from the regulator's perspective.

Why the DyGIST matters

Originally introduced in 2023, DyGIST represents a paradigm shift in how UK general insurers are expected to demonstrate resilience. Unlike previous point-in-time stress tests, DyGIST will simulate a sequence of escalating shocks over a short timeframe, testing not just solvency, but also firms' ability to adapt under stress.

The exercise is a full-spectrum test aimed to:

- assess the industry's solvency and liquidity resilience to a specific adverse scenario
- assess the effectiveness of insurers' risk management and management actions following an adverse scenario
- inform the PRA's supervisory response following a market-wide adverse scenario.

For insurers, we believe this is more than regulatory hygiene, it is a blueprint for strategic resilience.



What insurers should do now

Despite the 12-month delay, firms should stay on course and continue strengthening internal capabilities by actively investing in the following key areas:

Proactive measures	Potential implications	Potential benefits
Strengthen data infrastructure	Higher granularity and traceability of exposure data especially for natural catastrophe, casualty, cyber and long-tail liabilities.	Investing in data quality today lays the foundation for more robust and credible scenario analysis and stress testing. High-quality data enhances a firm's ability to generate insights, model risks accurately, and meet regulatory expectations.
Enhance dynamic modeling	Firms should simulate scenario propagation across multiple risk categories, including feedback loops (e.g., underwriting, claims, reputational impact, liquidity).	This would inform strategic capital allocation and help to test product mix under stress. It would also support risk-adjusted growth in new lines like parametric, cyber or specialty classes.
Embed stress testing in strategic governance	Senior management and boards should take ownership of stress test results.	Strong governance signals to regulators, investors, and rating agencies that the firm is well-managed and forward-looking, contributing to reduced capital charges and lower cost of capital.
Expand use of reverse stress testing	Firms should conduct more frequent reverse stress tests that could cause business model failure and test resilience beyond traditional actuarial limits.	Better visibility into existential threats leads to clearer strategy differentiation, smarter capital buffers, and earlier detection of market exit triggers.
Define realistic management actions	The PRA will expect firms to present plausible, executable recovery strategies (e.g., portfolio rebalancing, dividend deferral, capital raising) with timetables and triggers.	Firms with actionable contingency plans will respond faster to crises, reduce drawdowns on own funds, and maintain market confidence even under stress.



Next steps

The PRA will begin re-engaging with firms in September 2025 to provide updated guidance and expectations for the 2026 exercise. Forward-looking firms may want to consider:

- Conducting capability assessments to benchmark internal readiness against DyGIST criteria
- Integrating multi-scenario stress libraries into their reserving and ORSA functions
- Upgrading actuarial and catastrophe modeling platforms to support dynamic forecasting
- Mobilizing cross-functional working groups to bridge actuarial, risk, finance, and data teams
- Harnessing automation and advanced analytics to strengthen stress testing capabilities, drive efficiency, and deliver timely, data-driven risk insights.

DyGIST represents a paradigm shift in how UK general insurers are expected to demonstrate resilience.

Conclusion

The DyGIST is a signal of the PRA's evolving expectations that insurers must be agile, data-driven, and crisis-ready. Firms that act early can turn this requirement into competitive advantage, enhancing resilience, improving capital efficiency, and building stakeholder trust.

How Capco can help

Regardless of how far you have gone into your DyGIST journey, Capco can support through a range of options:

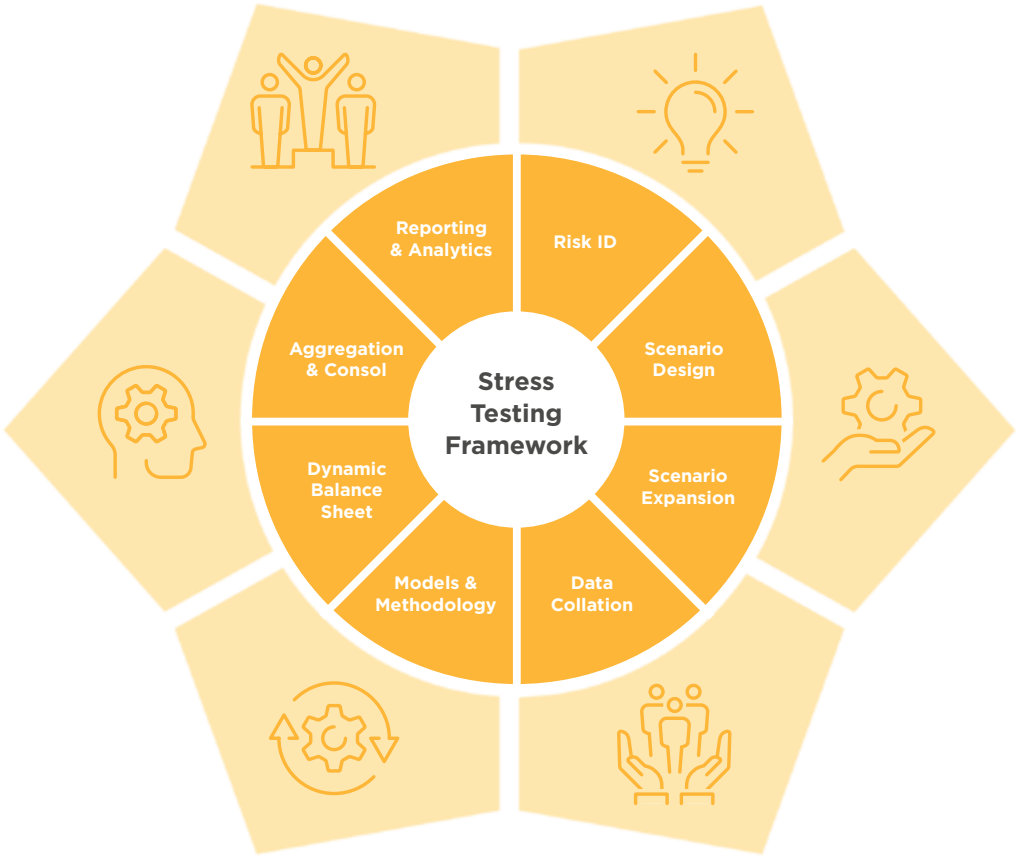
Designing and modelling of credible stress scenarios – Capco can collaborate with you to design plausible yet severe stress scenarios that capture idiosyncratic, market-wide and combined risk events (including reverse stress scenarios). Leveraging our accelerators and templates, we can help analyse and quantify the impact of adverse events on your capital and liquidity positions.

Gathering and analysis of historical data for calibration purposes – The quality and consistency of underlying data are critical to the robustness of your stress testing framework. Capco can help assess data integrity across systems, identify inconsistencies, and analyse historical data to inform forward-looking and hypothetical scenario assumptions for more accurate and credible model calibration.

Regulatory and industry benchmarking – Regardless of whether your stress testing framework is at a foundational or advanced stage, Capco can conduct a gap analysis against regulatory expectations and leading industry standards. We will work with you to achieve your desired maturity level.

Automation of risk-informed decision-making process – Stress testing outputs should be a core input into strategic decision-making. Capco can support you in automating stress testing workflows, developing real-time dashboards, and producing management information (MI) reports that enable proactive risk mitigation and integrated balance sheet management.

Stress Testing Offering



Insights & Management Actions	• Create MI reports to facilitate risk mitigation strategies • Build UI/Dashboards with advanced analytics • RWA and capital-planning strategies using stressed output • Portfolio and client strategies to ensure competitiveness and liquidity remains in times of stress
Regulatory Exercises	• Project management of regulatory exercises, incl. data gathering, template population, and submissions • Expert interpretation, and advice on methodologies • End-to-end support on taxonomy changes • Independent assurance procedures, validation, and challenge of results
Models & Methodology	• Expert interpretation, and advice on regulatory methodologies across all relevant risk types • Identification of gaps against regulations and best practice • Stress test model development and validation • Overlays and reconciliation of model inputs/outputs
Stress Testing Framework	• Design and implement stress testing frameworks integrated with firm's Risk Strategy, Risk Appetite, Capital and Liquidity Planning processes • Gap analysis on e.g., Institutions' stress testing guidelines • Organization Design & Location Strategy
Data & Architecture	• Optimize data quality & lineage for transparency of portfolio stress • Implement BCBS 239 principals for all levels of data granularity • Establish Stress Testing Data Framework (STDF) • Increase frequency & capacity for stress testing • System architectural design to achieve 'Stress-as-a-Service'
Scenario Design	• Capco-designed scenarios • Facilitate in-house design with firm's own internal experts • Independent assurance over forward-looking estimates • Creation of standardized inventory for on-demand stress across a range of scenarios and plausible risks.

Abhinav Jaipuriar

Alexander Croonen

Anna Cline

Ariana Szeto

Ben Harding

Bernard Cunningham

Betty Yip

Bianca Gabellini

Charlotte Byrne

Chris McNeely

Christian Bergner

Christoph Ruth

Daniel Outcalt

Dipanjan Naha

Donald Jennow

Edward Fielding

Femi Adeoye

Gabie Lang

Gaelan Woolham

Gaurav Mehra

Hardeep Mundair

Jamain Graveney

James Musgrave

Jamilia Parry

Jesús Pascual Camino

Kane Stavens

Mahir Alman

Marija Devic

Marina Cosens

Marina Drimili

Mehdi Rachidi

Mustakim Chowdhury

Natalie Igweze

Nathan Sowatskey

Nicola Goodeve-Docker

Oleander Yao

Pankaj Marwaha

Paul Carroll

Pascal Krautscheid

Peter Dugas

Petra Watkinson

Priya Mitra

Rakhima Gazizova

Reuben Karuna Nidhi

Richard Higgins

Richard Jackson

Saeed Patel

Shabnam Westcott

Shirley Low

Shiv Subramani

Shivaji Chakraborty

Siyi Liu

Sohrab Khan

Stephen McPherson

Thomas Mularski

Thanh Le Xuan

Viresh Tailor

Wesselin Kruschev

About Capco

Capco, a Wipro company, is a global management and technology consultancy specializing in driving transformation in the financial services and energy industries. Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on LinkedIn, Instagram, Facebook, and YouTube.

Worldwide offices

APAC
Bengaluru – Electronic City
Bengaluru – Sarjapur Road
Bangkok
Chennai
Gurugram
Hong Kong
Hyderabad
Kuala Lumpur
Mumbai
Pune
Singapore

MIDDLE EAST
Dubai

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
Glasgow
London
Milan
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto

SOUTH AMERICA
São Paulo

capco.com

CAPCO
a **wipro** company

© 2025 The Capital Markets Company. All rights reserved.

JN_1935