protiviti®
Global Business Consulting

COMPLIANCE INSIGHTS

The Compliance Playbook: Navigating the Financial Services Industry's Compliance Priorities in 2025

By Carol Beaumier and Bernadine Reese

As we approach the new year, the financial services industry again faces increasingly diverse and complex compliance risks, driven by the continued rapid pace of technological innovation, geopolitical tensions, and national and regional priorities. Understanding and managing these risks is essential for maintaining stakeholder confidence, ensuring operational resilience, and identifying and exploiting competitive advantage. Meeting this challenge in 2025 will be a true test of the industry's commitment and acumen.

Our 2025 priorities by region

In years past, we have categorised compliance priorities for financial institutions in various ways. We have grouped them under headings such as Uncertainty, Broader Risk Mandates and Traditional issues. Last year, we divided them into External and Internal. For 2025, we asked a larger than usual group of our Protiviti colleagues across the globe to help us identify the most pressing compliance issues in their markets – not a scientific survey, to be sure, but we believe a reliable one nonetheless. As we think it important to identify not only common areas of focus but also of divergence, we are sharing the regional groupings of the priorities. We do note, however, that there are far more common than divergent areas of concern and that in some instances the different priorities merely reflect a nuanced view of a common issue.

North America	Europe	APAC
Artificial Intelligence	Artificial Intelligence	Artificial Intelligence
Financial Crime	Financial Crime	Financial Crime
Privacy and Security	Privacy and Security	Privacy and Security
Operational Resilience	Operational Resilience (including DORA)	Operational Resilience
Third Party Risk Management	Third Party Risk Management	Third Party Risk Management
Consumer Protection	Consumer Protection	Conduct and Culture
Compliance Function Optimisation	ESG	FinTech
Resourcing	Virtual Assets	Compliance Function Optimisation
Heightened Uncertainty	Compliance Function Optimisation	Resourcing
Competitive Landscape	Resourcing	Economic Implications

In the following sections of this paper, we address the common priorities as well as specific regional priorities. We also comment on the importance of horizon scanning to maintaining an effective compliance program, a topic we have also addressed in past years. But before we address 2025, we want to reflect on how well we did with our 2024 projections.

2024 projections

For 2024, our groupings of External and Internal priorities included the following:

- **External**: Artificial intelligence, consumer outcomes, operational resilience, culture and conduct, sanctions, supply chain, crypto fallout, and convergence of financial crime.
- **Internal**: Compliance risk assessment, horizon scanning, risk in change, digital risk, compliance monitoring and resourcing.

We think regulatory guidance, enforcement actions and industry focus validated our 2024 issues, except for crypto fallout which we included last year in part because we thought we had given crypto short shrift in 2023. This year, we have included crypto/virtual assets as a priority for North America (under 'competitive landscape') and Europe. Let's see if we get it right this time.

Common 2025 priorities

Artificial intelligence

To no one's surprise, artificial intelligence (AI) is at the top of our list of compliance priorities. Seldom has a technology had such a pervasive impact on compliance risks. From fraud and deepfakes, anti-money laundering (AML) and sanctions, consumer protection, data privacy and operational resilience, AI is fundamentally changing how the financial sector operates. Given its potential, 41% of financial services firms surveyed in 2024 report that they are expecting to spend more than 10% of their digital budgets on gen AI alone.[1]

Different countries have taken distinctly different approaches to AI governance. These approaches, however, share one common objective: to reduce the risks of AI while allowing the industry to optimise its potential for enhancing both internal operations and customer engagement. In promulgating their expectations, global regulators are leveraging the core principles for AI as defined by the Organisation for Economic Co-operation and Development (OECD) and endorsed by the G20. These principles include respect for human rights, sustainability, transparency, and strong risk management. The risk-based approach being deployed by regulators, as set forth in the EU AI Act for example, seeks to address proportionally the perceived risks that specific AI systems pose to core values like privacy, non-discrimination, transparency, and security.

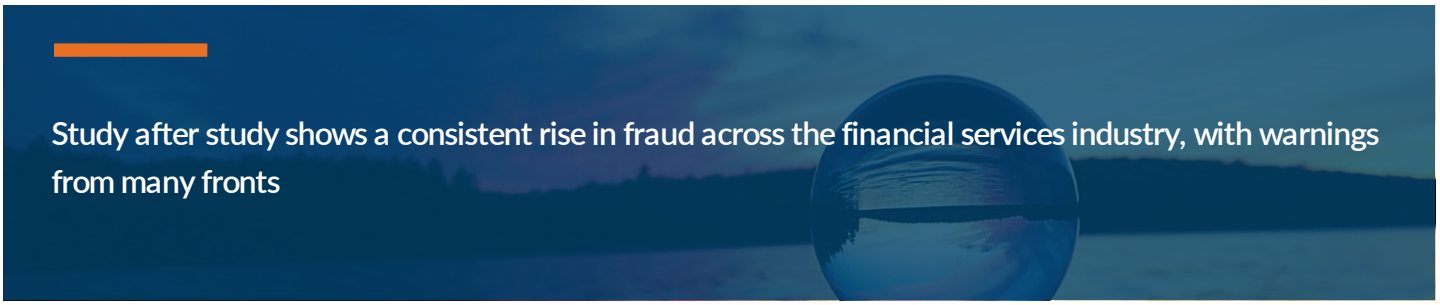
We expect to see financial services regulators develop specific rules, requirements, and guidance to ensure that their current regulatory frameworks enable them adequately to manage the risks posed by AI. Given the broad impact of AI, these regulatory requirements may be substantial and tailored to the needs of a number of regulators in each country. Maintaining some degree of global alignment would be welcomed by the financial services industry, but may be challenging to achieve given the considerable benefits of being seen as AI-friendly and an innovation frontrunner.

1 https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai.

Financial crime

The inclusion of financial crime on our list should not be a surprise since we have included it every year. Apart from the continued proliferation of new regulatory requirements and expectations, this year's inclusion was spurred not only from attention-grabbing AML enforcement actions in North America, the U.K., European Union and Asia-Pacific and the continuing pressure on the industry to deal with an increasingly complex and dynamic environment for sanctions and export controls compliance, but also by heightened concerns about fraud.

Study after study shows a consistent rise in fraud across the financial services industry, with warnings from many fronts, including a recent advisory from the Financial Crimes Enforcement Network (FinCEN), that artificial intelligence will heighten fraud risk. The increase in consumer fraud has also led to debates about who should suffer the losses– the consumer, the financial institution, or possibly the technology platform used to promote the scam. In the U.K., this debate led to a new rule requiring payment service providers to reimburse consumers for up to £85,000 in authorised push payment (APP) fraud, i.e., frauds perpetrated when individuals are deceived into sending payments under false pretences.



While many of the AML enforcement actions reminded us of the need to focus on the basics – customer due diligence/enhanced due diligence, risk assessment, comprehensive and timely transaction monitoring, adequate staffing and training, independent testing, management and board reporting, and a culture of compliance – the reality is that the industry will continue to lose pace with the bad guys (money launderers, sanction evaders, and fraudsters) unless and until it makes better use of advanced technologies, such as machine learning (ML) and AI, and predictive analytics to identify potential financial crime.

Privacy and security

As digital transformation continues to drive business innovation and operational efficiency, the importance of data privacy and protection remains in the forefront. Financial services regulators continue to take action and fine institutions for inadequate control when their responses to a cyberattack or significant data breach are inadequate.

The increasing frequency and sophistication of data breaches, including through the malicious use of AI, underscores the necessity for robust data protection measures. For example, generative AI tools enable attackers to make smarter, more personalised approaches and mean that deepfake attacks will become increasingly prevalent. Combatting such attacks may come down to a combination of more and continuing education awareness programs and use of AI to identify suspicious activity.

With the growing use of AI and ML in data management, regulators are paying closer attention to the privacy implications of these technologies. Modern privacy laws emphasise consumer rights, such as accessing, correcting, and deleting personal data. Protecting these rights is becoming more robust, with new requirements expanding on existing frameworks to give consumers greater control over their data. We expect regulators to increase their focus on consumer rights and consumer protection issues arising from data breaches.

Operational resilience

Regulators globally continue to implement regulatory changes and programs of work to ensure that financial institutions meet the resilience challenges of a digital age.

The most significant business disruption of 2024 was undoubtedly caused by the cybersecurity company CrowdStrike when a software update created widespread problems with computers running Microsoft Windows operating software. As a result, roughly 8.5 million systems crashed and were unable to properly restart in what has been called the largest outage in the history of information technology. Regulators were keenly interested in what happened and how affected companies dealt with the problem, bringing even more scrutiny on third-party risk management programs (discussed in more detail below).

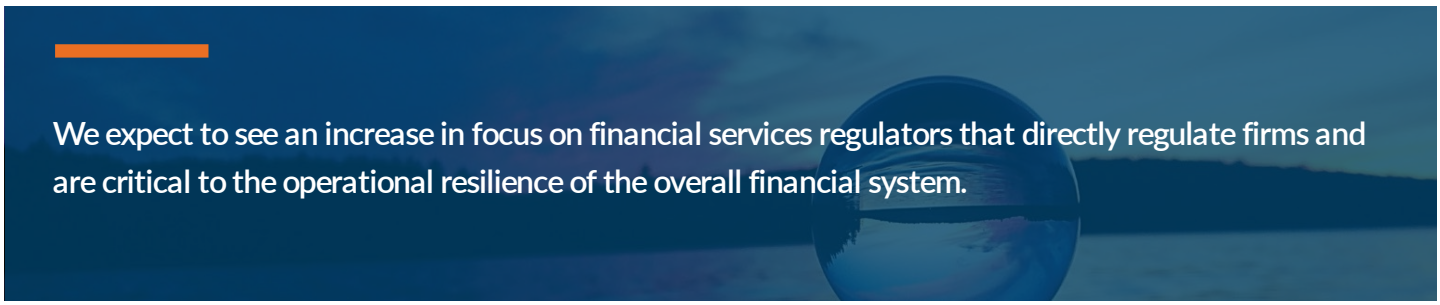
2024 has been the year of DORA (the EU's Digital Operational Resilience Act). Its implementation deadline of January 2025 means that affected financial institutions have been busy implementing the many changes relating to its key requirements.[2] Due to the inclusion of intragroup outsourcing arrangements within the coverage of DORA, many global financial institutions are finding that their operational resilience group policies need to be updated.

2 Key requirements include information and communication technology (ICT) risk management; ICT third-party risk management, digital operational resilience testing; ICT related incidents, information sharing and oversight of critical third-party providers.

Third party risk management

The financial sector increasingly relies on third parties for technology and other services, allowing it to embrace innovation and improve efficiency. Management and oversight of increasingly complex third-party arrangements is a growing challenge. In addition, large parts of the sector rely on a small number of third parties for key services. The impact of disruption to these services (e.g., the CrowdStrike incident) could spread through the financial system and threaten financial stability and market integrity or trigger a loss in confidence. This concentration is most notable in technology and cloud computing, where the dominance of a few Big Tech firms makes it challenging for individual financial services, particularly smaller institutions, to negotiate terms. As a result, exercising the oversight expected by regulators or demanding information or changes are more difficult to accomplish.

Increasing risk awareness is driving some regulators, e.g., in Europe and the U.K., to designate these significant third parties as critical third-party providers, bringing them into the regulatory perimeter. In the US, the Bank Service Company Act (BSCA) has for a long time allowed prudential bank regulators significant authority to oversee and regulate the activities of service companies that provide services to banks. We expect to see an increase in focus on financial services regulators that directly regulate firms and are critical to the operational resilience of the overall financial system. While individual firms remain responsible for operational resilience, we expect to see the regulators taking action to drive greater operational resilience measures from the technology and critical non- technology third party providers.

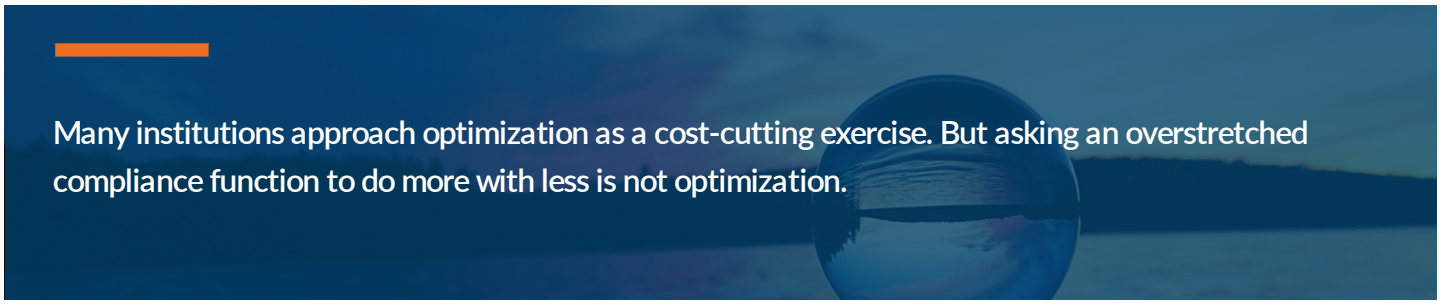


Consumer protection

A growing list of egregious failings by financial services companies for mis-selling financial products, misleading or mistreating groups of consumers and taking advantage of the information asymmetry that exists between firms and retail consumers has contributed to many regulators taking increasingly significant action to protect retail consumers. In the US, the Consumer Financial Protection Bureau (CFPB), which is expected to be reined in under the incoming administration, has pursued an aggressive agenda of consumer protection, targeting both traditional financial institutions as well as other providers of consumer services. Regulators, such as the U.K.'s Financial Conduct Authority, have imposed new "Consumer Duty"

requirements which require financial institutions to act to deliver good outcomes for retail clients. This outcomes-based requirement imposes an output-led standard rather than an internal process-led approach that has historically been used. In Australia, a number of consumer protection initiatives – including new scam protection laws, legislation focused on consumer protection on online platforms, and new draft crypto guidelines – highlight the priority placed by Australian legislators and regulators on consumer protection. Protecting consumers in the digital marketplace is also a high priority in Canada. We expect to see a continued focus from other regulators globally on consumer protection and mis-selling concerns.

2025 is also likely to bring greater scrutiny on how customers in financial difficulty and vulnerable customers are treated; how products are developed, tested and governed; and whether retail customers receive value from the products they buy. Disclosure of information to customers can no longer be considered sufficient – assessing whether customers understand such material also needs to be evidenced and assessed.



Compliance function optimisation

Financial institutions continue to grapple with optimising their compliance functions. Related to the Resourcing topic below, many institutions approach optimisation as a cost-cutting exercise. But asking an overstretched compliance function to do more with less is not optimisation. Those institutions that take this narrow view will ultimately fall short of meeting their compliance obligations and will spend even more money to make matters right. Compliance optimisation is about enhancing the overall effectiveness, efficiency, sustainability, and competitive edge of the compliance function. Any proposed changes to the compliance function should be viewed through each of these four lenses.

Resourcing

Effective compliance management requires investment in people. Far too often, as evidenced in regulatory enforcement actions, financial institutions bow to cost pressures and compliance departments, like other cost centres, become targets for cost savings. But even institutions that don't succumb to this ill-advised strategy often face challenges in recruiting, training and retaining the talent needed to be effective.

Solving this challenge requires thoughtful consideration of compliance options, some creativity and the right environment. For example, institutions could make better use of technology to perform routine tasks and/or co-source or outsource some people-intensive tasks, freeing up internal staff to focus on strategy and decision-making. Management could also broaden recruiting efforts to consider people with non-traditional backgrounds who have an interest in and can be trained on compliance requirements; this could involve partnering with local colleges and universities to identify promising candidates and offering internships. Most importantly, institutions need to demonstrate a strong culture of compliance and provide career paths for compliance professionals if they expect to attract and retain qualified talent.

Regional 2025 priorities

North America

The idiosyncratic issues for North America are largely the result of current circumstances in the US.

Heightened uncertainty

Even before the recent US presidential election, regulatory rulemaking and enforcement processes had been upended by a series of Supreme Court decisions which stripped agency heads of some of their authority to interpret law and enforce penalties for non-compliance. (Refer to this VISION by Protiviti in Focus for additional details.) As a result of these decisions, we can expect a more protracted rulemaking process and more litigation to challenge agency interpretations and enforcement.

The Trump 2.0 administration adds to the uncertainty. While the financial services industry is generally buoyed by the prospect of less regulation (including potential rollback of some existing requirements) and "lighter touch" enforcement, there are concerns that the Trump economic agenda could lead to interest rates remaining higher and to inflation. Further, a lighter regulatory touch at the federal level could lead to actions by states to address perceived gaps, adding to the industry's compliance challenges.

Competitive Landscape

Three other issues in the headlines are banking as a service (BaaS), open banking and crypto. For the last year, the banking regulators in the US have been issuing enforcement actions against BaaS providers stemming from their exposure to less-regulated crypto and payment companies. One result of these enforcement actions has been a levelling of the playing field between fintechs and banks by having the banks require them to improve their compliance programs.

In October, The Consumer Financial Protection Bureau (CFPB) finalized a new rule to facilitate open banking in the US. Banks have challenged the rule, arguing that it exceeds the agency's legal powers and could jeopardize consumer data security. Underlying these concerns is a view that the rule would hurt banks and help fintechs.

Even prior to the presidential election, there were indications that there would finally be legislation to establish a regulatory framework for crypto. Given recent announcements about the incoming President's choice to lead the Securities and Exchange Commission as well his appointment of a Crypto and AI Czar, the future outlook for crypto in the US is strong.

Exactly how the new administration, which has said it is committed both to innovation and curbing regulation, will address these issues remains to be seen.

Europe

While the top concerns for Europe mirror those of North America and APAC, the following stand out as reflecting differing regulatory priorities. We expect to see European regulators continuing a focus on environmental, social and governance (ESG) regulation as well as seeking to introduce and supervise crypto-asset regulation consistent with existing financial regulatory frameworks. The implementation of DORA and its supervision for the financial sector and critical third-party providers will be a key priority as will the transition of supervision to the new EU AML Authority during 2025.

ESG

The EU continues to develop and implement a substantial body of legislation as part of its sustainable finance strategy. The package of measures is extensive, covering corporate sustainability reporting, green bond regulations, ESG rating regulations, actions to address greenwashing and changes to the Sustainable Finance Disclosure Regulations, to name a few. In addition, the Corporate Sustainability Due Diligence Directive (also called the CS3D) will require in-scope companies to set up due diligence processes to identify adverse human rights and environmental impacts that arise in their own operations and those across all tiers of their supply chain. This move is expected to be far-reaching and demand much greater onboarding requirements.

The U.K. ESG position is emerging more slowly as U.K. regulators initially focus on corporate reporting through the adoption of the International Sustainability Standard Board (ISSB) disclosures and standards, the focus on greenwashing and sustainability disclosure regulations (including new investment labels) with ESG ratings regulations in final consultation and the publication of a policy statement on non-financial misconduct in the financial sector also expected in 2025.

Virtual assets (MiCAR)

The Markets in Crypto-Assets Regulation (MiCAR) establishes EU market rules for crypto assets that are not currently regulated by existing financial services legislation. Key provisions for those issuing and trading crypto-assets (including asset-reference tokens, e-money tokens and crypto-asset service providers) cover transparency, disclosure, authorization and supervision of transactions. organizational structures, business conduct rules, and consumer protection measures.

U.K. regulation of virtual assets is still in the legislative phase. The Financial Services and Markets Act 2023 and the proposed Property (Digital Assets) Bill set out further details of the regulatory landscape for crypto assets. The regulatory approach proposes leveraging current financial regulatory structures to oversee crypto assets, bringing a wider array of crypto assets and related activities into the scope of regulation, regulating a wider scope of activities, and enhancing financial crime standards.

APAC

The three concerns not included on the North American and European lists are conduct and culture, fintech, and economic implications. Drilling down into these issues suggests more commonality with other regions than might at first be apparent.

Culture and conduct are not new areas of focus for APAC. Numerous countries in the region have adopted or enhanced conduct and culture standards. In Australia for example, culture and conduct are also the driving forces behind consumer protection rules.

The APAC region has been a leader in permitting newer market entrants – crypto and other fintech firms – but there is a lack of regulatory uniformity that creates challenges both for regulators and for fintech firms looking to expand across borders. This is driving a push for greater regional cooperation and harmonization of regulatory standards.

While the medium and long-term economic prospects for APAC remain strong, current economic conditions (e.g., the slow recovery in China, persistent inflation in Japan, and depressed consumer spending in Australia) still loom heavily, with potential impacts on the financial services industry ranging from credit quality concerns to aggressive cost cutting.

Horizon Scanning

In prior years, we have talked about how critical horizon scanning is to compliance management. Identifying emerging risks and trends allows financial institutions to be more strategic, thoughtful and innovative in the way they address these issues, which in turn helps institutions avoid compliance problems and provides them with a competitive edge.

In a recent speech, former member of the board of the European Central Bank and New York State Department of Financial Services Superintendent Elizabeth McCaul talked about horizon scanning using an analogy to vision.

Ms. McCaul highlighted the importance of central, fringe and peripheral vision to both supervision and risk management. To paraphrase her words:

- Central vision is what's right in front of us, the risks of which we are all aware.
- Fringe vision is just outside of our central vision, the changes we see developing and beginning to have an impact.
- Peripheral vision is the wider risk landscape that includes the structural trends that could have a profound effect on business models and the environment in which financial institutions operate.

Peripheral vision issues, by their nature, are emerging risks which may arise over several years (such as the widespread adoption of online banking and financial services) or which can move from peripheral to central vision in a remarkably short time frame (for example, the emergence of AI). Most peripheral vision changes can be categorized as emerging from one of the following drivers of change: political, economic, social, technological, legal or environmental – the PESTLE analysis[3], a framework for exploring the external factors that may impact a business. Many of these drivers can have a multi-layered impact on business. But as Ms. McCaul points out, we need to use our "athletic capabilities to identify the peripheral vision risks." Her areas to watch include the potential reconfiguration of the financial value chain caused by big tech and other non-banking companies providing

3 https://pestleanalysis.com/what-is-pestle-analysis/

financial services, the impact of digitalization and social media on liquidity, and the rise of non-bank financial institutions. Our additions to this list include open banking and APIs, quantum, and supervisory technology (SupTech).

As we enter another year of change and uncertainty, we would recommend that the boards of directors and senior management of every financial institution evaluate their horizon scanning function against Ms. McCaul's standards.

And since we think we may be in for a very active 2025, check back with us mid-year when we plan to reassess the compliance environment.

About the authors

Carol Beaumier is a senior managing director in Protiviti's Risk and Compliance practice. Based in Washington, D.C., she has more than 30 years of experience in a wide range of regulatory issues across multiple industries. Before joining Protiviti, Beaumier was a partner in Arthur Andersen's Regulatory Risk Services practice and a managing director and founding partner of The Secura Group, where she headed the Risk Management practice. Before consulting, Beaumier spent 11 years with the U.S. Office of the Comptroller of the Currency (OCC), where she was an examiner with a focus on multinational and international banks. She also served as executive assistant to the comptroller, as a member of the OCC's senior management team and as liaison for the comptroller inside and outside of the agency. Beaumier is a frequent author and speaker on regulatory and other risk issues.

Bernadine Reese is a managing director in Protiviti's Risk and Compliance practice. Based in London, Reese joined Protiviti in 2007 from KPMG's Regulatory Services practice. Reese has more than 30 years' experience working with a variety of financial services clients to enhance their business performance by successfully implementing risk, compliance and governance change and optimizing their risk and compliance arrangements. She is a Certified Climate Risk Professional.

About Protiviti's Compliance Risk Management Practice

There's a better way to manage the burden of regulatory compliance. Imagine if functions were aligned to business objectives, processes were optimized, and procedures were automated and enabled by data and technology. Regulatory requirements would be met with efficiency. Controls become predictive instead of reactive. Employees derive more value from their roles. The business can take comfort that their reputation is protected, allowing for greater focus on growth and innovation.

Protiviti helps organizations integrate compliance into agile risk management teams, leverage analytics for forward-looking, predictive controls, apply regulatory compliance expertise and utilize automated workflow tools for more efficient remediation of compliance enforcement actions or issues, translate customer and compliance needs into design requirements for new products or services, and establish routines for monitoring regulatory compliance performance.