protiviti®
Global Business Consulting

COMPLIANCE INSIGHTS

Navigating the Financial Services Industry's Compliance Priorities in 2025: Mid-Year Checkpoint

By Carol Beaumier and Bernadine Reese

When we published our 2025 compliance priorities for financial services companies last December, we acknowledged that for a variety of reasons, understanding and managing compliance risks this year would be a true test of the industry's commitment and acumen. Among factors adding to the challenge this year, we noted the rapid pace of technological advancement, geopolitical tensions, and diverging national and regional priorities. Given the situation today, it seems appropriate to revisit the compliance landscape mid-year to evaluate whether our initial views were on target, whether there have been developments we did not predict, and how the industry is managing.

For reference, the chart below summarises the priorities we initially identified across three regions: North America, Europe and Asia-Pacific. The complete commentary on how we arrived at these priorities can be found here.

For our mid-year checkpoint, we thought it would be useful to gauge whether managing these priorities was proving to be in line with expectations (=), more (+), or less (-) challenging. Spoiler alert: none of the priorities is less challenging than we expected.

2025 Compliance Priorities for the Financial Services Industry

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 Optimization
Heightened Uncertainty	Compliance Function Optimisation	Resourcing
Competitive Landscape	Resourcing	Economic Implications

Below, we address the common priorities and then the regional priorities. We close with some thoughts on the accuracy of our initial outlook and how compliance departments are managing the challenges.

Common 2025 Priorities

Artificial Intelligence (=)

AI regulation has evolved as we expected thus far. The exponential growth in AI has been accompanied by increasing regulatory focus globally as regulators look to strike the right balance between encouraging AI innovation and maintaining financial stability and consumer protection. The European Union's AI Act, which came into force in August 2024, is the world's first comprehensive AI regulation, setting strict compliance requirements for financial services firms operating in the EU. It classifies AI systems into unacceptable risk, high risk, limited risk and minimal risk categories, with financial services firms primarily affected by the unacceptable risk and high-risk classifications. Financial institutions deploying high-risk AI systems must have appropriate controls, including risk assessments, that ensure AI models are free from bias, maintain human oversight of decision-making, ensure data quality and transparency, and implement cybersecurity controls.

After a failed effort to include a moratorium on state regulation, the Trump administration's One Big Beautiful Bill was signed into law on July 4. If and how the administration will continue to seek consolidating control over AI regulation remains to be seen. Nevertheless, the objective at the federal level remains unchanged: encourage AI innovation to support the US's competitive standing without imposing burdensome regulations.

Regulation of AI is, in fact, likely to remain contentious as governments and regulators look to balance the opportunities of the new technology with the need to control risks and to ensure that over-regulation does not put the country at a competitive disadvantage. A continued divergence of approaches should be expected.

Financial Crime (+)

Recent events have further complicated the financial crime compliance landscape. The US has sent mixed signals on its plans, , watering down its beneficial ownership registry rule and, after first enacting an 18 month freeze on enforcement actions under the Foreign Corrupt Practices Act (FCPA), issuing new FCPA enforcement guidelines this June. The new guidelines signal the US's intent to focus only on "serious misconduct" with an emphasis on cases that result in "economic injury to specific and identifiable American companies or individuals" or impact sectors that are critical to US national security. In a move that adds to compliance obligations and presents significant risks for non-compliance, the US also designated certain cartels as terrorist organisations as part of its multifaceted effort to impact their effect on drug trafficking, violence and border security.

On the global front, we are seeing less coordination with respect to new sanctions on Russia; considerable and widespread attention on the money laundering and sanctions risks of crypto assets and real-time payments; and an unrelenting focus on fraud risk coming from the media, regulators and financial institution customers.

Additionally, several local authorities are already focussing on preparation for upcoming Financial Action Task Force (FATF) reviews. Italy, Singapore, Canada, Mexico, China, Australia, the United Arab Emirates and the US are among countries that FATF assessment teams are scheduled to visit later in 2025 and in 2026. The pre-visitation period is often marked by increased regulatory scrutiny and a sense of urgency to address issues cited in a country's last evaluation report.

All of this is occurring as financial institutions continue to work to improve the efficiency and effectiveness of their financial crime compliance functions. See Compliance Function Optimisation below for more thoughts on this point.

Operational Resilience (=)

As expected, 2025 has so far been a big year for Operational Resilience with implementation deadlines for the EU's Digital Operational Resilience Act (DORA) package in January and the U.K.'s Operational Resilience requirements taking effect in March. DORA aims to harmonise information and communication technology (ICT) risk management, third-party oversight,

resilience testing and incident reporting across financial entities operating in Europe. DORA also covers oversight of critical ICT third-party providers to ensure financial institutions manage outsourcing risks effectively.

Operational resilience has become an area of increasing focus in APAC as well. The Australian Prudential Regulation Authority (APRA)'s CPS 230 Operational Risk Management standard takes effect this month, requiring financial institutions to enhance resilience with a strong emphasis on governance, critical operations and ensuring continuity of service.

Other countries in APAC, including Japan and Singapore, have also added to guidance or implemented operational resilience measures to minimise service disruptions.

Third-Party Risk Management (=)

The importance of third-party risk management has been a key lesson from the global operational resilience focus, with outsource arrangements and reliance on third party technology and business providers exposing many financial institutions to vulnerabilities. DORA requirements mandate stringent oversight of critical third-party providers, ensuring financial institutions mitigate risks associated with outsourcing at every stage from due diligence to ongoing monitoring. Other regulators have imposed similar provisions, often embedded within their operational resilience requirements. The impact of these provisions has been significant, particularly for multinational financial institutions that may rely on several hundred third parties and even fourth-party providers within their business. We expect third-party risk management to continue to be a challenging area of focus with the increasing risk of cyberattacks and the need to understand how AI will be used by third parties in dealing with organisations' clients and data.

Information Security and Privacy (+)

Many countries have witnessed a surge in cyberattacks and more sophisticated hacks this year. This is driving an increased focus on cyber resilience globally, with regulators in many jurisdictions including Australia, Hong Kong and Singapore taking further steps to improve cyber resilience and incident reporting. The increasing focus on operational resilience, AI regulation and fraud, in addition to growing geopolitical tensions which give rise to concerns about state-sponsored attacks, is driving a heightened regulatory interest in information security, data privacy and data governance.

Other regulators, such as those in the U.K. and Europe, have strengthened data protection and privacy requirements. The U.K.'s Data (Use and Access) Act is a key reform of the U.K.'s data protection regime, aiming to simplify compliance for organisations while strengthening the

"data protection by design" principle. The focus in Europe has been on enforcing the General Data Protection Regulation (GDPR) requirements, including a focus on cross-border enforcement and consistent treatment of the right to request data erasure.

Consumer Protection (=)

Consumer protection is an area that has seen significant diversity of approaches in 2025. We continue to see the U.K. adopting a strong regulatory stance on consumer duty, with a strong focus on vulnerable customers, monitoring customer outcomes and product governance. As part of the U.K. government's push to simplify regulation, we expect to see a continued focus on the need for financial institutions to achieve good customer outcomes but with fewer detailed and prescriptive rules. By contrast, in the US, the administration has made significant changes to the Consumer Financial Protection Bureau (CFPB) in 2025, focusing on deregulation, reduction in scope to a prescribed list of areas, reducing supervisory exams by 50% and refocusing enforcement activities. This significantly degrades the likelihood of consumer protection enforcement in the US, although state regulators have put the industry on notice that they plan to step in to address any void in federal enforcement.

There is also an increasing focus from many regulators including in the U.K., Australia and APAC on frauds and scams and the impact on retail customers. The U.K. has introduced a mandatory reimbursement requirement for authorised push payment frauds, which came into effect in October 2024 and which regulators consider to be working well. Due to the increased use of AI in frauds and scams we expect to see this trend continue, likely necessitating the need for AI to counter this threat through sophisticated identification of fraud attempts.

Compliance Function Optimisation (=)

The financial services industry entered 2025 committed to continuing its migration to smarter, more integrated and tech-enabled compliance models. The industry is motivated by a proactive desire to improve efficiency and by the defensive need to keep pace with an increasingly complex and fragmented regulatory environment and rapidly evolving threat landscape.

There are many examples of progress on both fronts. Risk assessments are being automated, allowing for more dynamic evaluations. AI, machine learning and advanced analytics are being used for broader transaction monitoring, sanction screening and fraud detection. AI is being used to develop and maintain regulatory inventories. More routine regulatory tasks, including compliance reporting, have been automated. Compliance teams have become better integrated with operational and cyber staff to share data, coordinate compliance efforts and eliminate redundancies. For many institutions, though, much remains to be done.

To continue making progress requires strategic investment and adequate resourcing. Both may be at risk in the current environment where economic uncertainty is driving some companies to defer investments and, along with the outlook for the regulatory environment (see section below), prompting others to cut compliance staff – to a point where compliance teams may be stretched too thin, resulting in overreliance on technologies. Failing to make the required investments and appropriately staff compliance functions is a missed opportunity and will delay and/or detract from the optimisation effort.

Resourcing (+)

Entering 2025, we identified two resourcing challenges: (1) recruiting and retention, and (2) the industry proclivity to target compliance departments for savings in reaction to cost pressures. Both are still challenges. What we didn't call out explicitly is what is becoming the biggest threat. Institutions in markets that are seeing "lighter touch" regulation and supervision may believe the current environment justifies cutting compliance staff below a level that would have been considered reasonable in years past. In some companies, compliance departments are already facing challenges supporting their staffing needs. History suggests, however, that institutions that cut compliance resources too deeply often pay a significant price for this decision, as we noted in The Survival Guide for Chief Compliance Officers in Uncertain Times.

Regional Priorities

North America (+)

The two regional priorities we identified for North America for 2025 related specifically to the uncertainty in the US: Specifically, the Trump administration's actions to reshape the regulatory landscape and their resulting impact on the competitive landscape. While it was clear from the start that the administration was intent on rolling back some regulation and easing enforcement activity, we did not fully appreciate the breakneck speed at which it would seek to replace the leaders of regulatory agencies (not generally a top priority for a new administration), how quickly it would move to reverse prior policies and support new ones (e.g., promotion of the crypto asset activity), or that regulatory agencies would be subject to significant staff reductions or, in the case of the CFPB, near elimination.

Although the administration's overall agenda may be clearer now, tremendous uncertainty remains. Prior rulemakings are still subject to agency reversal and legal challenge. Previously filed litigation against financial services companies continues to be withdrawn. Prior penalties assessed against financial institutions are being modified. Furthermore, the consequences of the administration's "10 to 1" rule – for every new regulation, guidance, or rule issued, agencies must identify and repeal at least 10 existing ones – remain to be seen. Bottom line: the future

regulatory landscape in the US is unpredictable.

The stated purpose of many of the changes made or under consideration is to enhance the competitiveness of US financial institutions. But a dearth of new regulation may result in the traditionally highly regulated segments of the industry, specifically banking organisations, finding themselves at a competitive disadvantage to newer market entrants such as fintechs that are not subject to as stringent requirements.

Europe (=)

We noted in the 2025 Compliance Priorities that ESG would be a priority in Europe given the robust EU agenda on sustainability matters and the expected pipeline of new regulation, including the Corporate Sustainability Reporting Directive (CSRD) and the Corporate Sustainability Due Diligence Directive (CSDDD). Surprisingly though, the emphasis has been on reducing the scope of ESG regulation. The Omnibus Simplification Package was introduced in February with the aim of streamlining EU regulations, and it removes around 80% of companies from the scope of the CSRD. This is consistent with the aim of regulatory simplification that is a common theme globally. ESG regulation in the U.K. was arguably less advanced than in the EU, so the overall impact of ESG regulation has been very limited, with all new changes thoroughly assessed through a cost-benefit lens.

However, aside from ESG, regulation in Europe continues to remain in focus, particularly in areas such as AI, and Europe sees the same uncertainties as other countries in terms of a drive to economic growth and regulatory simplification.

APAC (=)

Any financial institution that operates across APAC will tell you that dealing with the fragmented regulatory landscape is a big challenge. APAC, of course, is not untouched by global developments. That said, the current regulatory environment across APAC countries still seems to reflect our earlier outlook. This means few significant surprises beyond a likely uptick in the focus on AML compliance as several countries anticipate FATF reviews.

What did we miss?

We don't think we missed any specific challenge. We did, however, underestimate the extent of change that would occur in just months. Today, we think it is fair to say that one of the most pressing compliance issues facing the global financial services industry is the increase in regulatory fragmentation. Different jurisdictions continue to adopt divergent approaches to issues like digital assets, data privacy, ESG and more, making cross-border compliance more

complex. For global institutions, this means higher compliance costs, operational complexity, and legal/regulatory uncertainty.

For anyone old enough to remember the formation of the Basel Committee on Bank Supervision in the 1970s with one of its stated goals being the harmonisation of global standards and all the work since then to achieve it, this seems to be a big step backward.

How are compliance departments managing?

Best-in-class compliance departments recognise that, although it may sound contradictory, they need to respond proactively during this period of uncertainty. They are stepping up their horizon scanning activities to track agency publications, speeches and government agendas to anticipate changes. They communicate more frequently with executive management and their boards of directors to ensure the institution is prepared to deal with multiple regulatory scenarios. They are using this time to invest in long-term sustainable improvements to their compliance programs, leveraging AI and technology, and not just for quick fixes.

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 US 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 optimising 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 optimised, 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 organisations integrate compliance into agile risk management teams, leverage analytics for forward-looking, predictive controls, apply regulatory compliance expertise and utilise 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.

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for the 10th consecutive year, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI).

© 2025 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO-0725
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®