protiviti®
Global Business Consulting

COMPLIANCE INSIGHTS

Navigating 2026 Compliance Priorities: A Midyear Reality Check

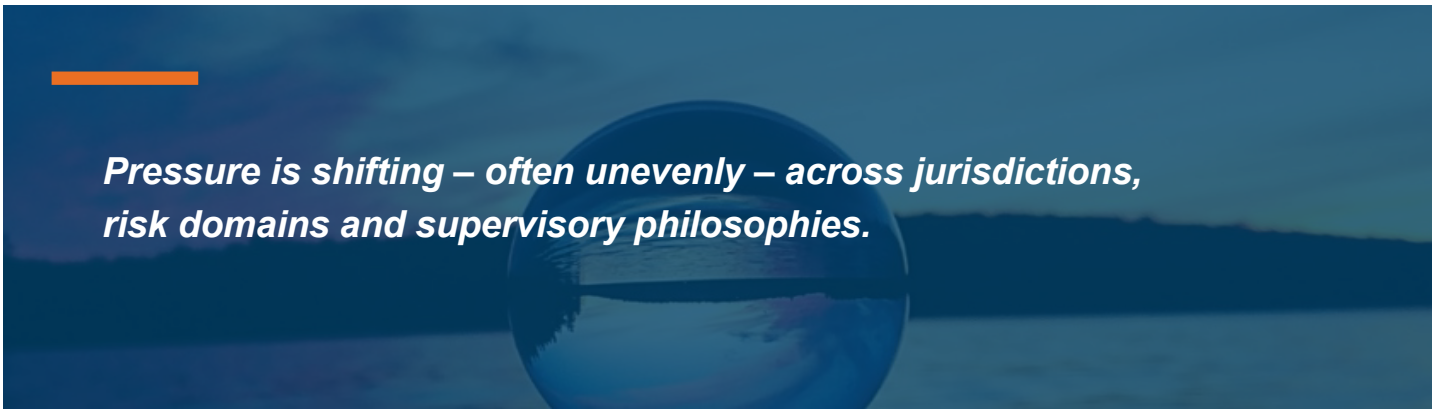
By Carol Beaumier and Bernadine Reese

As we set out to forecast this year's compliance priorities, we characterised **2026 as the most unpredictable year** in our experience. That view was driven by a convergence of forces: the profound transformation underway across the financial services industry, and shifting governmental and regulatory priorities.

At midyear, our assessment is holding. The year remains volatile. Pressure is shifting — often unevenly — across jurisdictions, risk domains and supervisory philosophies. What may appear, on the surface, as regulatory easing in some areas often masks a more complex reality: Expectations are being recalibrated, but exactly how and for how long is not always clear.

Against this backdrop, financial institution leadership must look beyond headlines and signals of "lighter touch" supervision to understand which risks are being de-emphasised and which are actually building — whether or not regulators currently are focused on them. Just as importantly, leaders can't lose sight of the fact that compliance decisions made today can have a bearing on regulatory examinations conducted years from now.

At midyear, the imperative is clear: Determine where to reinforce, where to reprioritise and where to hold the line, because missteps today may become problems tomorrow — not just from a regulatory perspective, but also with customers, because customer trust is increasingly paramount in a highly competitive landscape.



The core compliance stack

As context for any discussion of compliance priorities, it is worth reiterating that, notwithstanding current regulatory posture, the following all remain fundamental compliance issues:

- Artificial intelligence (AI)
- Digital assets and tokenisation
- Financial crime
- Geopolitical risk
- Market abuse
- Operational resilience
- Third-party risk management
- Information security and data privacy
- Cyber risk
- Consumer and investor protection
- Culture and conduct risk
- Compliance operating model, resourcing and technology tools.

What's different today is how some of these issues are being evaluated by regulators worldwide. Even in instances where the significance of some of these issues has been downplayed (e.g., the U.S. federal government's current stance on consumer protection), there remain underlying laws that still mandate compliance, and there are other stakeholders — customers, community and advocacy groups, state attorneys general, and state regulators and shareholders — that have a vested stake in how financial institutions perform.

The shifting regulatory perspective

What is driving changes in the regulators' outlook? The common reasons offered include the following:

- **Shifting politics:** In some jurisdictions, regulators, at the prompting of their national governments, have deemphasised issues such as ESG and DEI that are not political priorities or that, in the extreme, have become politically contested and subject to active government pushback.

- **Proportionality:** Regulators increasingly are acknowledging that a "one-size-fits-all" approach often imposes unnecessary burden on smaller and/or less complex institutions. This is leading them to advocate for a risk-based approach that better aligns supervisory expectations with an institution's risk profile and systemic significance.

- **Simplification:** Amid growing claims from multiple fronts that regulatory frameworks have become overly complex, costly and intrusive, regulators are undertaking programs to review and streamline rules, reporting and supervisory processes.

- **Prioritisation:** Regulators are shifting toward focusing on material risks, particularly those with clear financial impact and, in some jurisdictions but not all, potentially significant consumer harm implications. This reflects a goal to de-emphasise process or technical compliance and focus on risk issues that are perceived to be more significant.

- **Outcome-focused:** Related to the above, regulators are moving away from evaluating policies, procedures and frameworks to focus on actual outcomes and real-world impacts. This reflects a shift from an "if it isn't documented, it doesn't exist" mindset to one in which "the outcome supports that the controls are working."

- **Business friendly:** Governments and regulatory bodies alike are advocating for greater innovation and product development to spur economic growth but recognise regulation can be an obstacle. This is causing a shift toward a more hands-off approach to innovation, albeit one that still aims to maintain basic safeguards.

- **Competitiveness:** Regulatory recalibration is increasingly being framed in terms of global competitiveness, particularly as jurisdictions compare regulatory burden and industry performance. Policymakers are under pressure to ensure that domestic financial institutions are not disadvantaged when compared to their international peers, and that new market entrants that can spur competitiveness are afforded the opportunity.

The astute industry observer will note that, to varying degrees, we have heard all these reasons before. They sound compelling until there is an industry crisis, and then all bets are off, and senior managers and directors who thought they were making acceptable decisions at the time find themselves being held responsible for bad outcomes. Perhaps this time will be different, but we do not think that will be the case.

What our clients are telling us – globally

Despite a lack of global coordination — and in some cases, clear regulatory divergence — there are a number of consistent, cross-jurisdictional themes emerging in our client conversations. These themes cut across institutions of different sizes and types and across geographies, pointing less to local regulatory nuance and more to structural shifts in risk, technology and operating models.

Foremost among these themes are:

AI is moving into production faster than governance models.

Across virtually all markets, institutions are accelerating the deployment of AI. However, governance frameworks, model risk management practices and control functions are lagging implementation and creating a widening gap between innovation and oversight.

Clients are increasingly concerned that existing frameworks, which were designed for a different time, are not fit for purpose in a world of adaptive, opaque and continuous learning systems. Compliance functions are being asked to opine on risks (e.g., bias, explainability, consumer outcomes) before clear regulatory or even internal standards are fully established, increasing the likelihood that some decisions will need to be reevaluated once there is more regulatory clarity. Or worse case, Compliance is not even being brought into the AI discussion even when deployment has potential regulatory consequences.

And, lest we forget, the predictions for when Q Day will occur — the day quantum computers become powerful enough to break encryption algorithms — **keep getting shortened**. This means that before many institutions are prepared, quantum computing will increase AI risk by accelerating cyberattacks, supercharging model capabilities and breaking current security standards. For those institutions embracing digital assets, which are generally secured by cryptography, Q Day poses even greater exposure.

Fraud risk management pressure is mounting even in jurisdictions where AML intensity has eased.

Even in jurisdictions where AML scrutiny has lessened or become more targeted, clients consistently report that fraud risk concerns are intensifying. Key drivers of this escalating concern include real-time payments, synthetic identities and AI-enabled attack vectors.

This is creating a rebalancing of financial crime priorities, with fraud increasingly viewed as a more immediate, operational threat to both customers and institutions. In many organisations, this has exposed the long-standing fragmentation between fraud and other financial crime and customer risk functions, prompting renewed focus on an integrated financial crime framework, as **we discussed in a prior edition** of this publication.

Third-party risk has become a board-level resilience issue.

Third-party and supply chain risk, especially related to technology providers, fintech partners and critical service vendors, has escalated from a compliance and operational risk concern to a core enterprise resilience issue.

Clients increasingly are dependent on a small number of critical providers, raising concerns around concentration risk, operational continuity and outsourcing oversight. At the same time, the expansion of partner ecosystems has made end-to-end visibility of risk more difficult, particularly where fourth- and fifth-party dependencies are involved.

Geopolitics is fragmenting the rulebook.

Diverging national priorities are creating inconsistent, and sometimes outright conflicting, regulatory expectations. For global institutions, this is driving localised compliance models, higher operating costs and greater execution complexity, which has elevated geopolitical risk to a day-to-day compliance and strategy issue.

Talent fatigue is a compliance risk.

Amid cost pressures and, in many cases, headcount reduction targets tied to the lighter-touch supervisory environment and the adoption of AI, compliance functions are experiencing sustained capacity strain. What clients increasingly are describing is not just a resourcing issue, but a structural fatigue risk within control functions.

Experienced staff are being asked to cover broader mandates while often also being tasked with supporting transformation initiatives such as digitalisation and AI adoption. This has led to concerns around burnout, loss of institutional knowledge and a weakened second line of defence.

Taken together, these five themes point to an undeniable reality: Risk is accelerating and evolving faster than governance capacity and operating models; digitisation and AI adoption are leading to questions about long-held norms, such as the 3LoD model; and regulatory frameworks are not, in all cases, keeping pace.

What our clients are telling us – regionally

European Union

Across the European Union, clients describe a regulatory environment that is becoming more ambitious, prescriptive and fragmented than at any point in the past decade. While the EU continues to position itself as a global standard setter, the lived experience for institutions is one of accelerating regulatory volume, uneven national implementation and intensifying supervisory expectations. What stands out in our client conversations is not simply the breadth of new rules, but the operational strain created by overlapping reforms that touch every part of the risk and control landscape.

- **A dominant theme is the pace and complexity of the EU's digital regulatory agenda.** The AI Act, DORA, the Data Act and the Digital Services Act are all moving rapidly from legislative text to supervisory expectation, and clients consistently report that operational readiness is struggling to keep pace. The AI Act, in particular, is forcing institutions to redesign model inventories, documentation standards and risk classification processes before many have fully matured their existing AI governance. Supervisors also are signalling that "paper compliance" will not be sufficient, with early supervisory focus expected on DORA testing, ICT risk mapping and incident reporting. Clients describe a widening execution gap between regulatory ambition and operational capability as national competent authorities apply different interpretations and timelines.

- **Financial crime reform is accelerating.** While some global jurisdictions are easing AML intensity, EU clients report the opposite. The creation of the new EU Anti-Money Laundering Authority (AMLA), the expansion of the AML rulebook and the push toward greater data sharing are raising expectations across the bloc. At the same time, fraud risk is becoming a political priority. Instant payments legislation, combined with rising APP fraud and AI-enabled scams, is prompting supervisors to scrutinise fraud controls with the same seriousness historically reserved for AML.

- **Concerns about third-party and cloud concentration risk are becoming more prominent.** EU regulators are increasingly vocal about the systemic risk posed by dependence on a small number of cloud and technology providers. Under DORA, institutions must demonstrate not only robust oversight of their direct providers but also visibility into fourth- and fifth-party dependencies — an expectation many clients describe as operationally daunting. Boards are being asked to treat ICT outsourcing as a resilience issue rather than a procurement matter, and supervisory reviews already are probing concentration risk, exit strategies and the realism of contingency plans.

- **Regulatory fragmentation within the EU is increasing.** Despite efforts to harmonise rules and drive consistency through EU-level supervisors such as AMLA, clients report that national implementation remains uneven. Differences in supervisory interpretation — particularly around AI risk classification, DORA testing expectations, ESG disclosures and consumer protection — are forcing institutions to maintain country-specific compliance models. Many clients describe this as a growing structural challenge that adds cost, complexity and operational friction.

Looking ahead, our clients point to two emerging regulatory frontiers that are expanding the compliance perimeter. The Markets in Crypto-Assets Regulation (MiCA) is introducing a level of structure and scrutiny to crypto-asset markets that many institutions were not operationally prepared for, with new licensing, governance, custody and market-abuse obligations accelerating faster than internal readiness. At the same time, the EU's move to regulate ESG rating providers — bringing them under direct ESMA supervision — is reshaping how sustainability data is produced, validated and relied upon. Clients see both developments as early signals of a broader shift toward more intrusive oversight of digital and sustainability-related risks.

United Kingdom

In the United Kingdom, clients describe a regulatory landscape that increasingly is outcomes-driven and lighter on prescriptive rules, but with higher regulatory expectations. The UK's ambition to position itself as a globally competitive but high-standards jurisdiction is translating into reforms that emphasise governance accountability, operational resilience, consumer protection and digital market integrity. What our clients highlight most consistently is the shift in regulatory posture: Supervisors are increasingly focused on demonstrable effectiveness, not policy adoption, and institutions are experiencing a marked increase in data-led supervision, thematic reviews and rapid-cycle interventions.

- **A defining feature of the UK environment is the continued evolution of outcomes-based regulation**. The FCA's Consumer Duty has set a new benchmark for evidencing control effectiveness, with institutions expected to demonstrate — through customer-level data, management information (MI) quality, and board oversight — that their frameworks deliver good outcomes in practice. This standard is now permeating other regulatory domains, shaping supervisory expectations in conduct, resilience and financial crime.

- **Operational resilience is entering a more intensive supervisory phase.** With the UK regime reaching its 2025-2026 milestones, regulators are shifting from assessing design to testing execution. Institutions report increased scrutiny of impact tolerances, scenario testing and the credibility of assumptions around cloud reliance and cross-border service dependencies. Supervisors are now asking institutions to demonstrate how important business services can remain within tolerance during severe but plausible disruptions, signalling a clear move from framework-building to performance validation.

- **Financial crime reform continues to accelerate.** Despite political messaging about reducing regulatory burden, our clients consistently describe AML and fraud as areas of rising supervisory pressure. The UK's heightened focus on fraud — particularly APP fraud — is driving institutions to strengthen real-time detection capabilities, customer authentication and AI-enabled analytics, and regulators are swift to act when AML controls are not operating effectively.

- **AI governance has emerged as a distinct and rapidly intensifying regulatory priority.** Although the UK has deliberately avoided the EU's prescriptive approach, we consider the UK's principles-based model to be no less demanding with its focus on senior management accountability for AI oversight and governance. Supervisors are increasingly probing the governance of algorithmic decision-making, model explainability and data ethics, particularly in retail financial services where AI already is embedded in credit, fraud and customer-interaction processes. The government's evolving AI assurance framework is prompting institutions to formalise model inventories, strengthen validation standards and develop clearer lines of accountability for AI-driven outcomes. Our clients describe the challenge as "high flexibility, high accountability"; institutions must design their own governance standards and be prepared to defend them under supervisory scrutiny.

- **Nonbank financial institutions (NBFIs) are becoming a sharper focus for UK regulators.** This reflects concerns about systemic risk, market stability, and the adequacy of governance across investment funds, asset managers, insurers and other non-bank entities. Our clients note that the Bank of England and the FCA increasingly are scrutinising liquidity risk management, leverage and the resilience of market-based finance following recent episodes of volatility, including LDI-related stress. Supervisors are signalling that NBFIs must demonstrate stronger stress-testing capabilities, clearer escalation frameworks and more robust oversight of outsourced and delegated functions. Many clients describe this as a shift toward "bank-like expectations without bank-like rules," with regulators seeking to close perceived gaps in resilience and transparency across the broader financial ecosystem.

- **The UK is tightening expectations around third-party and cloud risk.** Although the UK has not adopted DORA, the Bank of England's forthcoming critical third-party-provider regime is prompting institutions to map material dependencies more deeply, strengthen exit and substitution strategies, and enhance cloud resilience testing. Many clients see this as part of a broader international convergence on cloud concentration risk, with UK supervisors increasingly coordinating with global peers.

Looking ahead, our clients point to two additional regulatory frontiers. Digital assets are moving toward full FSMA-based regulation, with new obligations around custody, market abuse and exchange oversight expected to crystallise through 2026. Meanwhile, ESG integrity is being reshaped by the UK's Sustainability Disclosure Requirements (SDR) and investment labels regime, which are driving new expectations around data quality, product governance and assurance.

APAC

As we often pointed out, with more than 150 countries, the heterogeneity of the APAC region presents a compliance challenge to financial institutions. That said, we are hearing a number of common areas of focus from our clients in the region. These include:

- Financial crime (AML and fraud/scam prevention)
- Third-party risk management
- Operational resilience
- Culture/conduct
- Data, AI and model risk governance
- Digital assets

The rationale for including these topics on a regional list may differ from country to country (e.g., Japan's focus on AML is influenced by an upcoming FATF review, while Australia's emphasis is more about the implementation of its Tranche 2 AML reforms). In fact, the regulatory approach in APAC is less about achieving regional harmonisation and more about principle-based supervisory pragmatism, national priorities, rapid response to innovation and increasing expectations for institutional accountability.

North America

From our Canadian financial institution clients, we are hearing a focus on several areas that have been identified as priorities by the authorities, including:

- Integrity & Security Risk (cyber, fraud, financial crime)
- Real Estate / Mortgage Risk (housing and CRE exposure)
- Liquidity & Funding Risk (market confidence, funding stress)
- Credit Risk (borrower stress, commercial and consumer)
- Impact of NBFI Risk (private credit, shadow banking spillover)

While keenly aware of the uncertainties affecting financial institution operations in the current environment and recommitting to a policy of smart supervision in which supervisory activity remains outcome-focused and is concentrated on the most significant issues, the Canadian approach to regulation and supervision appears firmly rooted in lessons learned from the past — especially when compared to the United States.

In the U.S., the current discussion is less about what supervisors will do and more about what they have explicitly chosen to de-emphasise. Regulators have moved to eliminate the use of reputation risk as a basis for supervisory criticism, formally prohibiting examiners from taking action against institutions on that basis and stressing that supervision should be anchored in objective, measurable risks tied to safety and soundness. At the

same time, there is a clear shift away from process-driven supervision: Agencies are raising the bar for supervisory findings and signalling that institutions will be evaluated less on the completeness of documentation or adherence to prescriptive processes, and more on whether outcomes pose a material risk to financial condition. This is part of a broader reorientation toward "material financial risks," with explicit direction to avoid excessive focus on procedures or control frameworks that do not directly impact financial stability. There are limited exceptions to this approach — sanctions compliance being one of the most notable.

The result is a supervisory posture that is narrower, more outcomes-based, and more tightly aligned to quantifiable measures of safety and soundness. For financial institutions, this creates both clarity and ambiguity: clarity in terms of what matters most to regulators, but ambiguity in terms of how far institutions can streamline controls, governance and risk frameworks without falling behind evolving expectations that may reassert themselves over time. Thus far, what we have seen is a significant drop in enforcement activity.

As U.S. regulators narrow their supervisory focus to core financial risks and step back from more subjective or process-driven areas, regulatory risk is declining as an industry concern. However, our discussions with industry leaders suggest they actually are expanding their view of risks. They are focused on cyber, fraud, AI, geopolitics and operational resilience, not as secondary concerns but as central drivers of financial performance and stability. The dominant theme we are hearing from them is not simplification, but convergence: Risks are compounding across technology, markets and operations in ways that traditional frameworks — and, in some cases, supervisory approaches — struggle to address.

The H2 2026 planning reset

To varying degrees in the first half of 2026, we have witnessed a lessening of regulatory pressure, but that does not mean regulatory risks themselves have diminished; in fact, as we have pointed out, some regulatory risks clearly are escalating. This means that the real pressure facing compliance programs today comes from determining how to respond in the best interest of the institution — for today and into the future — in an environment where signals are often fragmented and confusing.

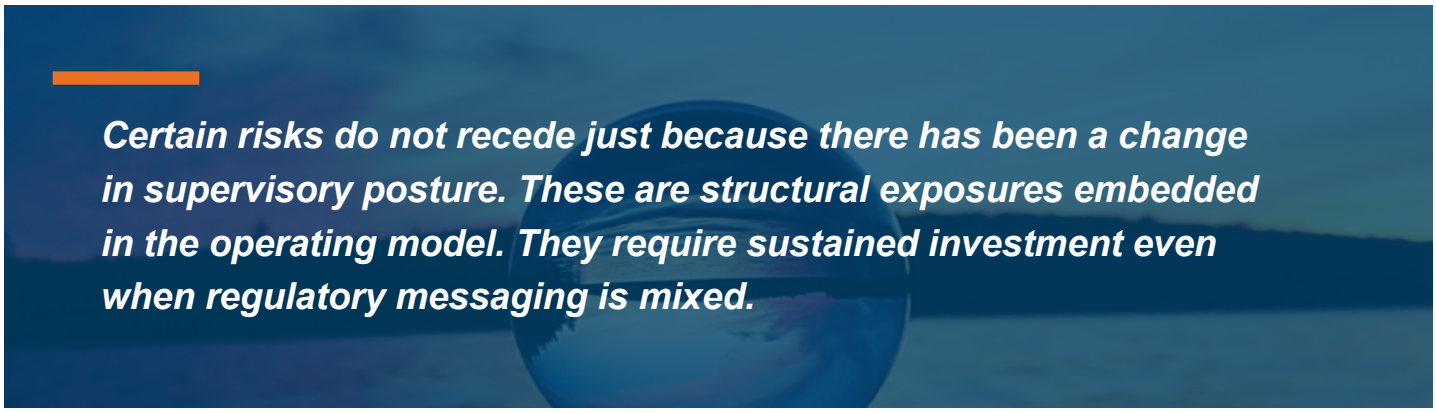
Given the current environment, our advice to financial institutions as they reassess their compliance strategies is:

Double down where risk is structural.

Certain risks do not recede just because there has been a change in supervisory posture. Financial crime, especially related to fraud, continues to intensify regardless of regulatory signals. AI deployment is accelerating independent of governance maturity. Third-party dependencies are deepening and becoming more complex, not stabilising. These are structural exposures embedded in the operating model. They require sustained investment even when regulatory messaging is mixed.

Reprioritise where regulatory narratives have shifted, but risk has not.

Proportionality, simplification and prioritisation are real themes, but they change the sequencing of work, not the underlying obligations. In practice, this means compliance leaders may have more flexibility in timing or approach but less tolerance for outcomes that fall short. Programs should be rephased to reflect where scrutiny is most likely to materialise next, but without assuming that de-emphasised areas are no longer relevant.



Certain risks do not recede just because there has been a change in supervisory posture. These are structural exposures embedded in the operating model. They require sustained investment even when regulatory messaging is mixed.

Hold the line in the face of false comfort.

Some of the most material risks for the remainder of 2026 will stem from areas where institutions incorrectly infer the pressure is off. For example, consumer protection and data privacy — even where politically or publicly de-emphasised — are based on statutory obligations and subject to scrutiny from a broader ecosystem, including customers, advocacy groups, and state or regional authorities. Regulator de-prioritisation does not mean de-risked.

Integrate — don't layer — across adjacent risk domains.

Fragmentation across fraud, AML, sanctions, cyber and customer harm is increasingly untenable in an environment where threats are converging. The rise in fraud and the increasing interplay among threat vectors require a more integrated approach. This is not about redrawing the organisational chart; it is about shared data, aligned risk assessment and coordinated response models.

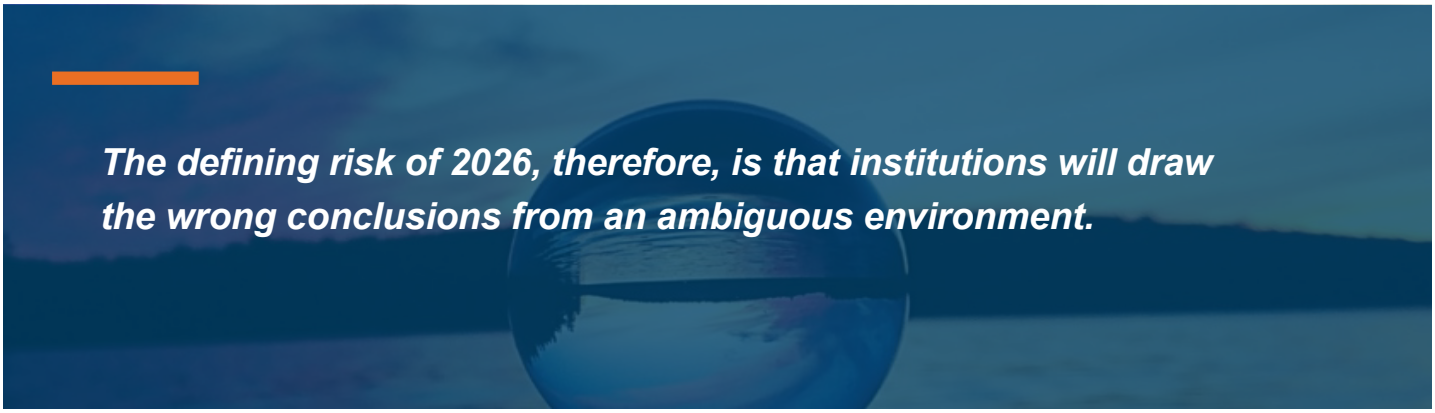
Reinvest in the compliance operating model.

The most underappreciated risk may be internal: capacity strain and talent fatigue. Compliance programs have been a target for cost-cutting. As mandates expand and expectations become more nuanced, compliance functions are being asked to do more with less, and often to support transformation at the same time. Addressing this requires a deliberate focus on skills, capacity planning and automation with proper governance.

This is not just an execution risk; it is a judgment risk. Without sufficient investment, even well-designed programs will struggle not only to operate effectively but also to interpret risk clearly and consistently in a fragmented environment.

The leadership imperative

Regulatory signals are more localised and more politically influenced than in prior cycles. The defining risk of 2026, therefore, is that institutions will draw the wrong conclusions from an ambiguous environment. But the underlying expectations — effectiveness, accountability and resilience — remain firmly in place.



This is where leadership must be explicit. Boards and senior executives increasingly are reliant on the sound judgment of compliance officers to interpret fragmented signals and translate them into defensible decisions. But that reliance is only as strong as the investment behind it.

If compliance functions are constrained — operationally or strategically — institutions are not just accepting execution risk; they are undermining the very capability they depend on to make the right calls. In 2026, compliance programs will not fail because institutions did too little; they will fail because organisations expected high-quality judgment without adequately enabling it, and as a result, misjudged what mattered most.

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 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 and 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.