

COMPLIANCE INSIGHTS

Top-of-Mind Compliance Issues for Financial Institutions in 2024

By Carol Beaumier and Bernadine Reese

In the ever-expanding landscape of financial services regulation, there are signs that the standard for compliance is shifting from a technical evaluation of how a financial institution implements laws and regulations to a more outcomes-based assessment that considers whether a financial institution has taken sufficient, proactive actions to prevent harm. With this shift comes the need for financial institutions, their boards and senior management, and their Compliance functions to have a clear and complete view of immediate and emerging risks and to ensure they have processes and controls in place to manage them proactively.

In years past, we have categorised compliance priorities for financial institutions under headings such as Uncertainty, Broader Risk Mandates and Traditional Compliance Issues. Today, it seems uncertainty and the disruption it brings have become the norm, as has Compliance's role in many other areas of risk management. This has resulted in the need for Compliance departments to self-evaluate continually whether they are optimising their operations to manage current and expected challenges. In turn, this has prompted us to group what we see as the 2024 top-of-mind compliance issues into two broad categories: External and Internal.

Compliance Priorities — 2024

External	Still Trending	New in 2024
1. Artificial Intelligence (AI)	✓	
2. Consumer Outcomes		✓
3. Operational Resilience	✓	
4. Conduct and Culture		✓
5. Sanctions	✓	
6. Supply Chain		✓
7. Crypto Fallout		✓
8. Convergence of Financial Crime	✓	
9. ESG	✓	
Internal		
10. Compliance Risk Assessment		✓
11. Horizon Scanning		✓
12. Risk in Change		✓
13. Digital Risk	✓	
14. Compliance Monitoring and Assurance		✓
15. Resourcing		✓

We have expanded our list this year from 10 to 15 priorities. There is no special significance to this number, just a nod to the fact that maintaining effective compliance programs at financial institutions isn't getting any easier. Additionally, as we have noted previously, our list is not intended to be all-inclusive. The priorities are not organised in any rank order and do not affect all types of financial institutions to the same degree, and aspects of the priorities clearly overlap.

We noted a LinkedIn post recently where a former compliance officer said he was not going to read any “top lists” this year unless the authors include the predictions they made in 2023 and prove they stood the test of time.¹ Fair enough, we say. So, before we elaborate on our 2024 expectations, we will revisit briefly our 2023 list.

In our list of the top 15 priorities for 2024, we have also indicated whether the priority is *still* trending, i.e., whether it appeared on last year's list or is new to the list this year. In several instances, “new” to the list does not mean the issue has not been a priority in the past but indicates that recent developments have moved it up the list for 2024.

¹ “It's tough to make predictions, especially about the future,” Jim Richards, *Anti-money Laundering — WTF?*, November 29, 2023: <https://antimoneylaundering.wtf/f/%E2%80%9CIt%E2%80%99s-tough-to-make-predictions-especially-about-the-future%E2%80%9D>.

2023 Revisited

Entering 2023, we expected the following to be priorities for financial institutions globally: financial stress; geopolitical tension; people challenges; regulatory hedging and blocking; emerging technology; data; environmental, social and governance (ESG issues); financial crime; privacy; and cybersecurity.² With the benefit of hindsight, we might have placed more emphasis on cryptocurrency, although it was mentioned in the context of regulatory hedging and blocking as well as financial crime. That aside, we think our 2023 list was on target and we stand behind our predictions. Several of the 2023 issues carry over to our 2024 list, some as they appeared in 2023 and others, as explained in the sections below, using different terminology as issues have continued to evolve.

2024 External Issues

Whether in the context of back-office operations, customer-facing services, risk management or compliance, no issue garners more attention today than **AI**. While animated debate continues among governments, advocates for the responsible use of technology, and the financial services industry — including participants at the Bletchley Park AI Safety Summit in November 2023 — as to how AI should be regulated, financial institutions are grappling with the opportunities and risks of AI. Along with board members and senior executives, compliance officers need to understand quickly the technology to manage the compliance risks it poses. Compliance officers will play a key role in determining the controls needed in business and operations applications of AI to meet local regulatory requirements as well as data governance and model requirements. They would also be well-advised, as discussed further below, to consider how AI can be used to improve the efficiency and effectiveness of the Compliance function.



Compliance officers will play a key role in determining the controls needed in business and operations applications of AI to meet local regulatory requirements as well as data governance and model requirements.

² “The evolving complexity of financial institution compliance: Top compliance priorities for 2023,” *Compliance Insights*, Protiviti, December 2023: www.protiviti.com/sites/default/files/2023-07/newsletter-top-compliance-priorities-for-2023-protiviti.pdf.


Consumer protection measures are the mainstay of retail compliance. Therefore, compliance officers will be tracking the rollout of consumer protection measures in the U.S., Australia, Europe, Hong Kong, Singapore and other jurisdictions. After trying for more than 20 years, with limited success, to ensure that financial institutions “treat customers fairly” and then identify and manage “conduct risk” relating to customer interactions, the UK’s Financial Conduct Authority has received new powers (through the Consumer Duty) to regulate **customer outcomes** — ensuring that regulated firms, effective July 2023, must act to deliver good customer outcomes for retail customers (including vulnerable customers). This regulation raises the bar for UK financial institutions. Another recent example of outcomes-based regulation comes from the Australian Securities and Investments Commission (ASIC), which has fined multiple financial services firms for poor customer outcomes, including misleading statements and financial promotions, unfair contract terms, overcharging customers, and other poor pricing practices.

Operational resilience, with cybersecurity as one of its linchpins, continues to be high on regulators’ agendas globally, although regulatory approaches and expectations may differ by country. Given the interconnectedness of the financial services industry, there is increasing focus on dependencies on critical third parties, outsource arrangements and vendors that play critical roles in delivering important business services and on which financial institutions rely to achieve resilience. Being able to monitor and oversee such third parties, which may number in the hundreds for individual firms, is a key area of focus. In July 2023, U.S. prudential regulators issued their long-awaited *Interagency Guidance on Third Party Relationships: Risk Management*, and in December 2023 the Financial Stability Board released a tool kit for enhancing third-party risk management and oversight; these are just two examples of recent regulatory guidance. While operational resilience programs are generally not managed by the Compliance function, Compliance nonetheless will continue to play a key role in ensuring that all regulatory requirements and standards are met.



Operational resilience, with cybersecurity as one of its linchpins, continues to be high on regulators’ agendas globally, although regulatory approaches and expectations may differ by country.

Conduct and culture — and the increasing impacts they have on regulatory risk — will be a focus for compliance officers in 2024. Whether it is the regulation of non-financial misconduct or the proposed mandatory disclosures to encourage diversity and inclusion in the UK, or publication of a consultative *Culture and Behaviour Risk Guideline* by Canada’s Office of the Superintendent of Financial Institutions (OSFI)³ outlining outcomes for which firms are accountable and emphasising how a sound culture and proactive management of behavioural risks contribute to good outcomes, an organisation’s culture has never been more important. Compliance officers know that sustainable and embedded implementation of regulatory requirements is effective only when reinforced by senior management action and a supportive company culture. The many impacts of culture on financial misconduct and poor customer outcomes are increasing regulatory focus on board effectiveness, governance, senior management accountability, and remuneration and incentivisation. In Hong Kong, regulators have introduced new requirements for remuneration design and claw backs, and in Australia, financial services firms also need to evidence a board-level view on risk culture.⁴ In examples of “practice what you preach,” two U.S. regulators, the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC), are currently under scrutiny for culture and conduct lapses related to, respectively, ignoring a hostile work environment and deficient vetting of a senior-level hire.



The many impacts of culture on financial misconduct and poor customer outcomes are increasing regulatory focus on board effectiveness, governance, senior management accountability, and remuneration and incentivisation.

With a slowing, but not stopping, issuance of Western **sanctions** against Russia, industry and regulatory attention has shifted from implementing the sanctions to evasion and enforcement. Regulators across the globe have published studies and guidance on evasion techniques, such as the May 2023 joint release by the U.S. Financial Crimes Enforcement Network (FinCEN) and the U.S. Bureau of Industry and Security (BIS), as well as the UK National Crime Agency’s (NCA) November 2023 warning on the use of gold to evade Russian sanctions. Contrary to what we have witnessed in the past, where it has taken regulators and other enforcement bodies years to build and report cases of sanction evasion, we are already seeing a steady stream of reporting of


³ *Culture and Behaviour Risk Guideline*, Office of the Superintendent of Financial Institutions, Government of Canada, February 2023: www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/cbrsk_dft.aspx.

⁴ *How financial firms can prepare for the 2024 regulatory landscape*, EY, December 2023: www.ey.com/en_gl/banking-capital-markets/how-firms-can-respond-to-the-2024-regulatory-landscape.

Russian evasion — a clear sign of the importance Western governments are placing on trying to cut off evasion channels.

These cases highlight the need for financial institutions' Sanction Compliance departments to be highly engaged and coordinated with their counterparts in transaction monitoring, trade operations and cyber risk management, among others, in order to identify and report evasion. (More about this is found below in our discussion of the convergence of financial crime.) Financial institutions simultaneously need to consider other lessons learned during the early days of the Russian sanctions and modify and enhance their sanctions compliance programs accordingly. Finally, it must be noted that geopolitical tensions across the globe, including U.S.-China relations and the Middle East conflict (including Iran's potential role), remind us that while much of the sanction attention in the last two years has been on Russia, compliance risk overall is far more pronounced than it has been in recent history and carries with it significant enforcement and reputation risk.

When we consider managing **supply chain** risk, we generally think about manufacturers and retailers and not about financial institutions. Apart from the credit issues that may stem from supply chain disruption, a financial institution's supply chain also presents compliance risks including corruption, fraud, export controls and sanctions, ESG requirements, and labour law anti-human trafficking compliance, among others. This requires financial institutions to make sure they are considering these issues as part of a comprehensive third-party risk management program, and in light of stepped-up constituent and regulatory interest, the latter should include supply chain certification requirements that are required in some jurisdictions.



Compliance risk overall is far more pronounced than it has been in recent history and carries with it significant enforcement and reputation risk.

Who would have thought that — following the conviction of FTX's Sam Bankman-Fried, the multibillion-dollar settlement with Binance and the conviction of its CEO, Changpeng Zhao, amid other crypto industry scandals — there would be optimism about the crypto world? But this is exactly what has happened. The two cases are quite different, of course: The FTX case involves the mishandling of customer funds, while the Binance case is based on alleged money laundering and sanctions violations. With these cases nearly resolved, there is optimism that this chapter of **crypto fallout** is behind us and that investors can now feel more confident that

bad actors will be punished. Crypto prices, in fact, recovered in 2023 following the devastating losses incurred in 2022. The future, however, is not as clear and rosy as some would like to believe. While jurisdictions across the globe (including Japan, Singapore, Hong Kong, Dubai and the UK) continue to welcome cryptocurrency companies and have developed and implemented regulatory regimes to supervise them, the United States remains a bystander, with no defined regulatory regime and where the future of crypto currently depends on the outcome of SEC litigation and on the political will (thus far lacking) for the Congress to act. For now, the disparate national frameworks governing crypto activities will continue to challenge financial institutions and their compliance personnel.

Financial crime has been a perennial issue on our listings of compliance priorities. New anti-money laundering (AML) requirements are never lacking, and recent events, as discussed above, have elevated the focus on sanctions compliance. Beyond these core pillars of financial crime, we are seeing a push toward the **convergence of financial crime** — a view that includes not just AML and sanctions, but also anti-bribery and corruption, fraud, cybercrime, and market abuse, among other areas. We have seen this push before, but progress has been slow and mixed at best. Two factors may now serve as catalysts to develop more integrated financial crime functions: an overarching, global concern with the proliferation of fraud and cybercrime, and the availability of innovative technologies. Compliance officers will be expected to be the architects of these integrated financial crime-focused Compliance functions and should increasingly expect regulators to ask about their plans and progress.



We expect continued focus on the development and implementation of ESG strategies and policies in many countries.


In our June 2023 edition of *Compliance Insights*, we argued for the need for the Chief Compliance Officer (CCO) to step up and play a key role in the adoption of **ESG** strategies. At COP28's Finance Day in December 2023, we saw how the financial sector remains a vital mechanism for initiating and sustaining change. We expect continued focus on the development and implementation of ESG strategies and policies in many countries, although in some the political realities and costs of adopting green and net zero policies are causing less progress than might have been expected from a climate emergency. We expect that regulators will continue to develop and refine disclosure regimes, and the introduction of the first of the Statements from the International Sustainability Standards Board will bring hope that greater global alignment

around disclosure standards and requirements can be achieved. Financial regulators, including those in Europe, the UK, Canada, Japan, Hong Kong and Singapore, will continue to focus on developing and refining climate change stress tests, anti-greenwashing measures and definition of the “S” (social) components, as well as on developing the sustainable finance markets. The planned or expected adoption of reporting and disclosure standards in various jurisdictions, including Europe and the United States, will set further compliance expectations.

2024 Internal Issues

Today’s CCO might be forgiven (at least temporarily) if she says she is too busy dealing with everyday fires to think about optimising the Compliance function. But we all know that not upgrading compliance operations only adds to the view that everything is a firefight. In the following sections, we offer some observations and recommendations for the busy CCO.

No competent CCO would argue with the premise that a **compliance risk assessment** is foundational to building an effective risk management program. Yet often, the process of developing the risk assessment seems to take on more significance than the results, and results may be obsolete by the time the risk assessment is finalised. This is an area ripe for innovation. CCOs would be well-advised to consider how they can use AI to develop a regulatory inventory (the first step in performing a risk assessment) and a risk control library and use technology to automate the risk assessment process to make it dynamic rather than static.

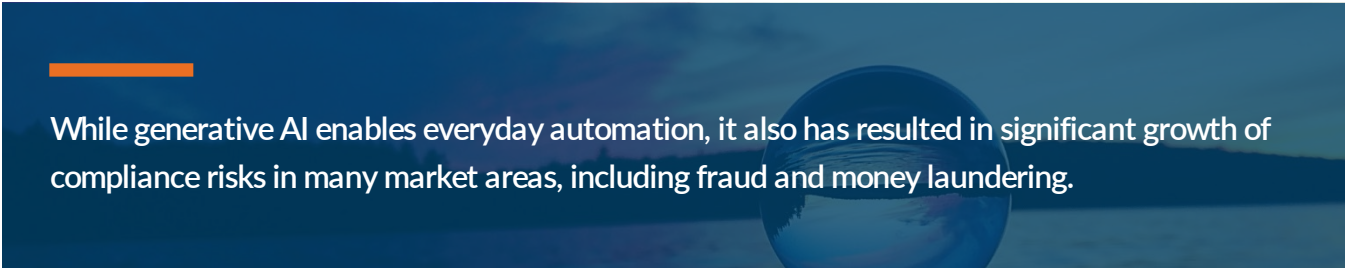


CCOs would be well-advised to consider how they can use AI to develop a regulatory inventory and a risk control library and use technology to automate the risk assessment process to make it dynamic rather than static.

For a risk assessment to be dynamic and for financial institutions to demonstrate to their regulators that they are attuned to and proactively considering the impact of emerging compliance risks, financial institutions need a **horizon scanning** function. This function uses a variety of sources to perform a systematic examination of new or potential areas of compliance risk, effectively communicates the expected impacts, and keeps the appropriate people in the institution informed of developments to allow for better preparedness and implementation. In smaller, less complex financial institutions, the CCO may be able to carry out this function, but in larger, more complex and multinational institutions, horizon scanning is a full-time job that may require a team of people to be effective.

Given the dynamics of the regulatory environment, a CCO, or a senior member of her team, also needs to be an expert at **risk in change** — the process of guiding organisational change from design and preparation through implementation. The costs of poorly managed change are many: missed deadlines, rework, increased costs, flawed implementation, and — in the case of regulatory requirements — potential violations of law, financial penalties and other regulatory actions. Change itself is a risk to financial institutions, and being an effective change agent is a core competency of a CCO. This requires the CCO to understand the change culture (including pain points and other obstacles) within her institution, develop a change management framework that works with the culture, continually prioritise the change issues facing the institution, and champion the change culture.

Risk in change extends beyond the implementation of new requirements — it also has a direct impact on issues management. While compliance issues may arise anywhere in an institution, the Compliance function has final sign-off (or, in some instances, penultimate sign-off before review by internal audit) on whether compliance issues have been appropriately resolved. This requires that Compliance identify all open issues, effectively challenge and sign-off on remediation plans, approve related communications (e.g., to customers or regulators), monitor implementation status, and confirm that the resolution satisfies regulatory requirements and expectations. It may also require Compliance to conduct training on new or revised processes and develop and implement monitoring regimes to protect against recurrence. How well institutions manage the adoption of new requirements and remediate open issues can significantly impact a regulator's assessment of the Compliance function and the effectiveness of the CCO.



While generative AI enables everyday automation, it also has resulted in significant growth of compliance risks in many market areas, including fraud and money laundering.

Over the past few years, we have consistently called out **digital risk** arising from emerging technology as a key focus area for CCOs. Prior to the launch of ChatGPT in November 2022, it would have been hard to foresee the extent to which technologies such as AI would be at the top of a CCO's agenda barely a year later. While generative AI enables everyday automation, it also has resulted in significant growth of compliance risks in many market areas, including fraud and

money laundering. Last year we referenced Forbes' Top Technology Trends in 2023;⁵ the 2024 Forbes list includes generative AI, sustainable technology and cyber resilience. (See sidebar.)

While some technology trends (such as cyber resilience) are not new, the rapid deployment of AI and advanced technologies is increasing the risks in these areas. Constant review and updating of cyber defences is required and resilience in the face of a cyberattack becomes critical. The 2024 trends also include “phygital,” which refers to the greater alignment and interaction of the physical and digital worlds. For example, as virtual reality and augmented reality become more mainstream, CCOs may consider how this technology can help with training. Digital twin usage has already become more widespread in operational resilience arrangements. Similarly, widespread adoption of advanced technology in society and financial services will need to be underpinned by quantum computing speeds and capacities.

Top technology trends for 2024

- Generative AI — everyday automation
- Phygital convergence
- Sustainable technology
- Cyber resilience
- Quantum computing


Source: “The Top 5 Tech Trends In 2024 Everyone Must Be Ready For,” *Forbes*, Sept. 11, 2023:
www.forbes.com/sites/bernardmarr/2023/09/11/the-top-5-tech-trends-in-2024-everyone-must-be-ready-for/?sh=1b9c15549a6b.

With more “next gen” technology now available, **compliance monitoring and assurance** is undergoing a transformation from an “optional” activity to one that adds value and insights. The focus on outcomes rather than process in areas such as consumer protection is leading to a focus on outcomes testing by the monitoring function. CCOs who focus monitoring on issues they have assessed as higher risk, use appropriate technology to automate monitoring controls, bring in expertise to conduct thematic reviews, and align their monitoring with the controls testing in the first line and internal audit reviews will be well-placed in managing the firm’s regulatory risk.

⁵ The 2023 list included (1) Artificial intelligence and machine learning, (2) Metaverse, (3) Use of digital twin technology in a digitally editable world, (4) Widespread adoption of DeFi, and (5) Increasing connectedness in the IoT.

Last but never least is **resourcing**. There is an oft-repeated pattern in Compliance functions: Ramp up when regulators criticise the compliance efforts of the financial institution, and ramp down as soon as the previously identified issues have been resolved. While a Compliance function should not staff for crisis mode, fluctuations in resourcing are not the solution either. Leveraging technology to the extent feasible, Compliance functions should be staffed with a core team of skilled and experienced individuals to meet business-as-usual needs. The team also should have the capacity to scale by borrowing personnel from other departments and/or engaging consultants or temporary staff when the situation demands it.

This, of course, is not as simple as it sounds. First, there needs to be agreement on what the business-as-usual needs are given the expanding role of Compliance as we have described it here and in previous publications. Next, there needs to be recognition that the current staff may need to be upskilled to meet current and future challenges. Finally, depending on a flex model requires pre-planning to identify the resources that will be added as needed. And for anyone who believes that innovative technologies will do away with the need for compliance personnel, we say, “Not a chance.” The more innovative technologies like AI blur the distinction between reality and fantasy, the more important the human touch becomes to ensure institutions satisfy not only the letter but also the spirit of laws and regulations.



The more innovative technologies like AI blur the distinction between reality and fantasy, the more important the human touch becomes to ensure institutions satisfy not only the letter but also the spirit of laws and regulations.

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, 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 our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2023 *Fortune* 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.