



The evolving complexity of financial institution compliance: Top compliance priorities for 2023

Ask an executive from most any company anywhere across the globe what her biggest concern is for 2023 and she is likely to say “uncertainty” — notably, uncertainty about how geopolitical tensions, national elections and their aftermath, and economic conditions will affect the business as well as uncertainty about the company’s ability to adapt to the post-COVID work environment.

Financial institutions’ compliance functions will not be spared from these and other uncertainties in 2023. These unpredictable circumstances will add to an already crowded compliance agenda — an agenda that includes continually expanding expectations for Compliance (which we have termed “Broader Risk Mandates”) as well as unrelenting, traditional compliance challenges. To frame the compliance challenges we expect financial institutions to face in 2023, we have grouped our Top 10 priorities into three categories: Uncertainty, Broader Risk Mandates and Traditional Compliance Issues.

Our list is not intended to be all-inclusive, nor are the priorities included in any rank order. These priorities do not affect all types of financial institutions to the same degree and aspects of the priorities clearly overlap. We believe there should be no comfort in the fact that our list is shorter than last year — 10 vs. 13 priorities — because many of the 2023 priorities are multi-dimensional and will require extensive effort

by Compliance and other financial institution process owners to address them effectively.

Compliance Priorities 2023

1. Financial stress
2. Geopolitical tension
3. People challenges
4. Regulatory hedging and blocking
5. Emerging technology
6. Data
7. ESG
8. Financial crime
9. Privacy
10. Cybersecurity

Uncertainty

In 2023, uncertainty will affect compliance functions because of financial stress, geopolitical tension, people challenges and regulatory hedging and blocking.

Financial stress

Financial stress will raise issues of engagement with and treatment of consumers, credit risk, and fraud, among other considerations. The longer and more severe the impact of inflation, the more vulnerable consumers and the higher regulatory concern will be.

Following on the heels of regulators' inquiries and concerns about how financial institutions engaged with consumers during the worst of COVID-19 and recent regulatory issuances¹ requiring financial institutions "to act in good faith, avoid causing foreseeable harm, and enable and support customers to pursue their financial objectives," customer dealings during a period of financial stress will be closely watched by regulators. As rising interest rates affect retail customers' ability to service their debt, Compliance and other financial institution stakeholders will need to pay careful attention to how they manage attendant issues such as forbearance, collections, complaint handling and credit bureau reporting.

Financial stress will also likely focus more attention on credit products such as Buy Now, Pay Later (BNPL) which are already being challenged by regulators over concerns that their terms and conditions are not clearly disclosed, and the products are not well understood by consumers. Compliance will need to monitor regulatory developments closely since additional regulation of BNPL products is likely in several jurisdictions. And, as we have learned repeatedly, financial stress is one of the key reasons people commit fraud. Increasing fraud risk should prompt financial institutions to revisit their fraud scenarios to ensure that they provide adequate coverage for themselves and their customers.

Geopolitical tension

Geopolitical tension remains high. While Russia's invasion of Ukraine and the global response thereto may be the event that comes to mind first, it is but one example of geopolitical risk. BlackRock has, in fact, identified three geopolitical themes that will shape the post COVID-19 world: US-China relations, deglobalisation, and inequality, all of which contribute to geopolitical fragmentation.² The result of this fragmentation is countries lining up on different sides of an issue. In the case of the Russian-Ukraine war, one group of countries has issued an unprecedented and growing number of economic sanctions and trade restrictions against Russia, and another group is demurring — publicly or privately. This situation has not only upped the ante for sanctions compliance including the identification of sanctions evaders but also has broader implications for anti-money laundering compliance and reputational risk management. In the months immediately following the invasion of Ukraine when sanctions were being issued on an intraday basis, compliance organisations were stretched to interpret and apply myriad sanctions and to advise management on the broader risk implications. The lessons learned from this experience should provide the playbook for handling future, similar situations.

People challenges

For those who thought time would solve the people challenges that have garnered so much attention since companies began trying to get people to return to the office, an article³ by futureworld suggests the challenge may be much more difficult than envisioned. The article shares 12 "things you need to know" about the new generation of employees (as well as the new generation of customers) that futureworld calls "Coronials." There are some positives on this list, including digital savviness and destruction of the gender pay-gap. There are concerns as well, including

¹ See, for example, the U.K.'s Financial Conduct Authority's (FCA) [Consumer Duty](#) standard and the U.S.'s Consumer Financial Protection Bureau's (CFPB) changes to its [Unfair, Deceptive, or Abusive Acts or Practices](#) authority.

² Geopolitical Risk Dashboard, BlackRock, www.blackrock.com/corporate/insights/blackrock-investment-institute/interactive-charts/geopolitical-risk-dashboard.

³ "Meet the Coronials' 12 Things You Need to Know About the Customer of the Future," by Neil Jacobsohn, futureworld, <https://futureworld.org/wp-content/uploads/2022/10/Meet-the-Coronials-Your-Customer-of-the-Future.pdf>.

disloyalty. However, the most striking of the 12 points may be #11: “They will lead us, they will guide us,” which is elaborated as follows:

The power has shifted forever. Young people are taking a leading role — they understand the technology and the digital world better than we do. . . They have a deeper understanding of the fusion between the digital and the physical world that businesses must tap into, if they want to be successful into the future.

12 Things You Should Know About Coronials

1. They will be 100% digital.
2. Work is an output, not a place.
3. They are extremely health conscious.
4. They want to be heard.
5. They are impatient, demanding and disloyal.
6. They are digital nomads.
7. For them, speed is non-negotiable.
8. They will destroy the gender pay-gap.
9. They will view teams differently.
10. They will be all about relationships.
11. They will lead us, they will guide us.
12. They have the “Youth-Tech” factor.

Like it or not, businesses, including compliance functions, will need to adapt to this new reality, and the sooner they realise this the more effective they will be in designing their future organisations. Further, compliance functions will need to compete within their own organisations and with other companies and industries to attract and retain the best talent. In the near term, compliance functions may be especially challenged to find resources with experience dealing with the impacts of a stressed credit market, particularly since it’s been more than a decade since the last credit downturn and the labour market is so tight. More broadly, however, in an environment where

having an impact may be the most important reason for selecting a job, compliance functions have at least two strategic advantages: (1) Compliance personnel are influencers. They serve as the conscience of their organisations and advocate for their organisation’s customers and (2) Compliance’s mandate is broad, and the work is never boring, as evidenced by the breadth of topics addressed here and in prior editions of our Top Compliance Risks. Compliance functions should use these advantages in their recruiting and retention efforts.

Regulatory hedging and blocking

The final category under uncertainty, regulatory hedging and blocking, is unique to the financial services industry. On one level, this occurs routinely when political agendas change — often moving from an aggressive enforcement agenda to light touch regulation and back again. Increasingly, though, it happens because regulators are struggling to keep up with innovation and technological advancement. We have seen this happen with cryptocurrency, the cloud, use of social media and messaging systems and, recently, with the metaverse. In the interest of not stifling innovation, some regulators may be slow to establish their expectations or may respond piecemeal. Frameworks may differ from country to country. These circumstances force Compliance personnel to monitor closely developments in all the jurisdictions within their and their customers’ geographic footprints and put compliance officers in the unenviable position of trying to predict regulatory reactions in order not to delay or impede business strategies. So long as financial institutions continue to innovate, regulatory hedging and blocking may be inevitable, but opportunity seems to exist for greater global regulatory coordination on innovations that are broadly affecting the financial services industry. The industry should encourage this collaboration.

Broader Risk Mandates

We see a continuing trend for Compliance to be drawn into wider risk mandates and be required to consider areas outside of traditional Compliance skill sets and experience. For 2023, these broader risk mandates include emerging technology, data, and environmental, social and governance (ESG) initiatives.

Emerging technology

Emerging technology is changing the financial services business model. The capabilities and capacities brought about by the cloud and big data analytical software mean that many compliance teams already are having to catch up with the business. And innovative technology continues to be adopted at an accelerating rate as noted by Forbes⁴ in its article on the biggest technology trends for 2023. Compliance teams will need to understand innovative technologies and the regulators' current thinking, which as previously noted may be subject to

Forbes' Five Biggest Technology Trends in 2023

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

jurisdictional variances, to allow them to evaluate the risks and impacts and to provide suitable challenge of new products or technologies before they are adopted. Senior management who will be required to provide oversight and challenge the risk implications of such innovative technologies will also look to Compliance functions to provide a view of the regulatory position.

The rapid evolution of technology has seen an explosion of structured and unstructured data in financial services. Increasing cloud adoption will drive this trend further in 2023 and with this growth

will come an increasing focus on the regulatory obligations for data privacy and confidentiality. At the same time, many regulators are increasing demands for data from financial institutions to enable a more data-led approach to regulation that allows greater use of analytics to deepen their understanding of regulatory and market issues and proactively identify risk events as they emerge. Recent examples include the U.K.'s focus on data monitoring and review as part of its Consumer Duty obligations and the data challenges that ESG is bringing. Compliance teams will be expected to assist with responding to increased demand for regulatory reporting and to serve as regulatory liaisons, meaning that they will need to understand how the data is sourced, its quality, how it is used and stored, and what story it tells the regulator.

Continuing cost pressures on Compliance will also continue to drive a focus on how Compliance innovates and optimises technology in areas ranging from regulation mapping, call monitoring, automated checks and surveillance and transaction monitoring systems.

ESG

ESG initiatives remain high on the agendas for regulators and financial institutions. While this focus is expected to continue to evolve in 2023, the geopolitical impacts of the war in Ukraine and the Russian response to weaponizing fossil fuel supplies have added further complexity and a short-term focus by many governments on finding alternative energy sources or extending the existing fossil fuel sources such as coal power stations. ESG regulation continues to develop rapidly with a focus on sustainability beyond net zero into biodiversity and deforestation.⁵ The social agenda is gaining momentum with the U.K. Prudential Regulation Authority (PRA)/FCA, for example, publishing requirements relating to diversity and inclusion and the publication of a

⁴ "The 5 Biggest Technology Trends in 2023 Everyone Must Get Ready For," by Bernard Marr, Forbes, September 26, 2022, www.forbes.com/sites/bernardmarr/2022/09/26/the-5-biggest-technology-trends-in-2023-everyone-must-get-ready-for-now/?sh=ac2f11555d90.

⁵ Proposal for a Regulation on Deforestation-Free Products, European Commission, <https://ec.europa.eu/environment/forests/deforestation-proposal.htm>.

⁶ Dear CEO Letter, Financial Conduct Authority, July 19, 2021, www.fca.org.uk/publication/correspondence/dear-chair-letter-authorised-esg-sustainable-investment-funds.pdf.

⁷ SEC Charges BNY Mellon Investment Adviser for Misstatements and Omissions Concerning ESG Considerations, May 23, 2022, Securities and Exchange Commission, www.sec.gov/news/press-release/2022-86.

⁸ ASIC Acts Against Greenwashing by Energy Company, October 27, 2022, Australian Securities and Investments Commission, <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-294mr-asic-acts-against-greenwashing-by-energy-company>.

social taxonomy in the EU in 2022. We expect to see Compliance functions being involved in many aspects of ESG frameworks and in particular, the regulatory focus on greenwashing through a variety of regulatory statements⁶ and enforcement actions^{7,8} is likely to draw Compliance into key decisions in

65% of global financial institutions are investing in new technology to assist with measuring and reporting on ESG risk and issues, compared with 50% of organisations across industries, according to data from Protiviti's 2022 Finance Trends Survey.

this area. Compliance functions will need to help the business understand new and emerging ESG regulations, integrate ESG considerations into many compliance matters including reviews of marketing materials, and consider and be ready to explain how the organisation's ESG strategy impacts areas of regulatory concern.

Traditional Compliance Issues

While there are countless traditional compliance issues that require the attention of Compliance, including the consumer protection issues discussed above, our focus here is on three that are at the top of the list every year.

Financial crime compliance

Financial crime compliance, as in years past, will continue to be one of the most dynamic areas of compliance. Barring another major geopolitical event, we expect the 2023 focus to shift from sanctions to anti-money laundering and counter terrorist financing (AML/CFT). The new year will bring new laws and regulations, continued high profile enforcement, and new and added focus on underlying crimes.

On the regulatory front, a few examples of evolving AML/CFT compliance frameworks include:

- Nearly two years after the enactment of the Anti-Money Laundering Act of 2020, the U.S. has a long way to go to implement the law fully.
- The EU continues its efforts to harmonise standards across its member countries and move to launch a regional authority.
- The U.K., no longer subject to EU requirements, has adopted new post-Brexit AML requirements.

The enforcement landscape also continues to evolve with non-traditional players such as cryptocurrency companies, casinos and real estate agents grabbing some of the headlines from banks and broker-dealers. This is a trend that we expect will continue into 2023, although large traditional organisations are likely always to be in the crosshairs.

Recent events, including the war in Ukraine, the global focus on ESG and a never-ending series of cyber events, have resulted in increased regulatory focus on precedent crimes such as kleptocracy, ecoterrorism, human trafficking and cyber intrusions. This requires a financial crimes compliance function to demonstrate how its compliance program addresses these concerns — from risk assessment to know your customer (KYC) to monitoring for suspicious activity.

All the above comes against a backdrop of continued efforts to innovate AML/CFT compliance that are progressing at different paces due to a variety of reasons, including the risk appetites of institutions and regulatory encouragement or lack thereof. With the dual mandates of comply and innovative, 2023 will be yet another busy year for financial crimes compliance.

Data privacy

The exponential volume of data in financial services is driving increasing concerns from global regulators about data privacy and ensuring that customers are aware of how their data may be used. Gartner has estimated that 65%⁹ of the world's population will be covered by legislation like the EU's [General Data Protection Regulation \(GDPR\)](#) by the end of 2023 as countries including Canada ([Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#)), China ([Personal Information Protection Law \(PIPL\)](#)) and all European member states have adopted

⁹ Gartner Report: 65% of the World Protected by Data Privacy Legislation by 2023, www.compliancejunction.com/gartner-report-65-of-the-world-protected-by-data-privacy-legislation-by-2023/#:~:text=A%20report%20released%20by%20Gartner%2C%20Inc.%20has%20estimated,virtually%20in%20the%20Americas%20and%20EMEA%20this%20week.

data privacy legislation. Several U.S. states have implemented similar requirements, including California ([California Consumer Privacy Act](#)), Virginia ([Consumer Data Protection Act](#)), Colorado ([Colorado Privacy Act](#)) and New York ([Stop Hacks and Improve Electronic Data Security Act](#) (SHIELD)). The growing sources of requirements and variation by jurisdiction mean that global financial institutions are required to manage varying data privacy requirements simultaneously. The willingness of regulators to take enforcement action (including significant fines) creates higher stakes for institutions. Compliance will be working with legal and data privacy teams to track these various requirements and manage local requirements in IT systems that are increasingly global in reach.

Cybersecurity

Cyberattacks remain a growing criminal activity and financial services regulators are focusing on their operational resilience impacts. The European Union Agency for Cybersecurity (ENISA) has highlighted a number of new and emerging cybersecurity threats in its recent [publication on the 2022 threat landscape](#). It notes how the number of cybersecurity incidents since the Russian invasion of Ukraine has been driven by geopolitical factors and “a wave of hacktivism” resulting from that conflict. While ransomware and malware are on the rise again, phishing is the most common access point for hackers, according to the report. The report also raises concerns about cybersecurity at a time when machine learning models are increasingly becoming a target and artificial intelligence (AI)-enabled disinformation is a growing trend. Regulators will continue to focus on developing and testing cybersecurity defenses, the operational resilience of critical business services, incident reporting and senior management’s understanding of IT risks such as cybersecurity.

One final note before we close out our 2023 list of compliance priorities: This year, we did not call out third-party risk management (TPRM). That’s not because it is not important, but because it is pervasive. It affects so many aspects of a financial institution’s processes and operations — how it secures and deals with clients, how it processes and manages data and how it uses myriad technologies to carry out its day-to-day activities — that TPRM, which is a global regulatory priority, needs to be embedded throughout an institution.

Are there other priorities we could have included? Yes, that is always the case. And with the elevated level of uncertainty, we would not be surprised to see changes to the priorities throughout the year. But that is the nature of Compliance: Priorities are broad and growing and their significance is impacted continually by internal and external events.

About Protiviti’s Financial Services Industry Practice

Protiviti’s global financial services industry practise has served more than 75% of the world’s largest banks and many of the largest and mid-sized brokerage and asset management firms, as well as a significant majority of life, property and casualty insurers. The FSI practise provides support to teams across Protiviti’s portfolio of solutions, including regulatory compliance, risk management, internal audit, technology, cybersecurity, data privacy and sustainability.

Contacts

Carol Beaumier
Senior Managing Director
Risk & Compliance
Protiviti – New York
carol.beaumier@protiviti.com

Bernadine Reese
Managing Director
Risk & Compliance
Protiviti – London
bernadine.reese@protiviti.co.uk

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, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the [2022 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.

© 2022 Protiviti Inc. PRO-1222-107214-IZ-ENG
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®