protiviti®
Global Business Consulting

Compliance Priorities for 2022 in the Financial Services Industry

As we consider the compliance challenges that will be top of mind for financial institution compliance officers in 2022, one thing is very clear: More and more often, they are being expected to play a significant role in managing risks that extend beyond what we have traditionally considered the purview of compliance. Coupling this reality with ongoing innovation, both in the industry and in supervisory approaches, means that attracting and retaining a broader complement of skills and experience are critical to the success of any compliance department.

To reflect this evolving environment for compliance, we present our views on the 2022 compliance priorities in three broad categories: **the broader risk mandate**, **traditional compliance issues** and **impacts on the compliance department**, recognising that the lines between and among these categories are inevitably blurred.

Our list, which is not in any rank order, is not intended to be all-inclusive and the priorities discussed do not affect all types of financial institutions to the same degree. In 2021, our list included 12 top compliance priorities – flippantly, one per month. This year, we have added a bonus 13th priority. We think most, if not all, of the issues discussed are relevant to financial institutions globally.

The broader risk mandate

The broader risk mandate includes risks which usually have been owned by the first line or other second line functions but today require deep involvement from the compliance department.

Environmental, social and governance (ESG): ESG touches many different areas within a financial institution: strategy, reporting, sustainable lending and investing, supply chain, human capital management (including corporate culture, and diversity, equity and inclusion), and corporate governance among them. Unlike more mature areas of risk (such as cybersecurity,

which is discussed below), many financial institutions may not have established clear responsibility for their ESG obligations. And compliance officers are not likely raising their hands to add more to their already long list of responsibilities – particularly something as complex as ESG. However, once regulators began promoting ESG agendas and issuing related regulations, it was inevitable that compliance departments would find themselves key participants in financial institution ESG programs. As regulatory expectations globally become clearer, compliance departments will need to detail their ESG responsibilities and accountabilities, including, if they have not done so already, standing up ESG compliance functions to measure and monitor compliance efforts and test the integrity of reporting across all dimensions of ESG. They will also need to play a significant role in coordinating an ever-growing and potentially conflicting multinational framework of laws and regulations.

Compliance Priorities in 2022

- ESG
- Cybersecurity
- Cloud
- Operational resilience
- Third-party risk management
- Crypto
- Culture and conduct
- Vulnerable customers
- Use of AI in decision-making
- Financial crime
- Data-led supervision
- Innovation/cost reduction
- The people agenda

Cybersecurity: The connections between cybersecurity and compliance are many. Cybersecurity is about protecting data and complying with myriad data protection laws and regulations; cybersecurity is regarded as an ESG issue, under the "S" pillar; cybersecurity is a core principle of operational resilience; cybercrime is a financial crime; an institution's response to dealing with a cyber-intrusion ransomware request may give rise to sanctions concerns; and cyber breaches may trigger reporting requirements. These all mean that compliance departments must share responsibility with their colleagues in technology to ensure their institutions have adequate cybersecurity programs by, for example, providing advisory support on breach notification requirements, the parties who should be notified and what remediation may be required. This has never been more important than it is now, when cyber attacks dominate the headlines on a continual basis.

Cloud: Financial institutions increasingly have been moving critical services to the cloud, but many have found that their cloud strategies have been met with questions and challenges from their regulators. Regulators already expect financial institutions to be able to articulate clearly how responsibility and accountability for cloud security requirements are shared with their cloud providers. Led by the European Union and the U.K., regulators have also expressed concerns about the reliance of financial institutions on a small number of cloud providers and the potential resiliency issues this raises, suggesting that cloud providers themselves may be subject to resiliency standards and testing in the not-too-distant future. Given the regulatory interest and possibility of additional regulation of cloud providers, compliance departments play

an important role in advising institutions on regulatory expectations for cloud management today, and these expectations continue to evolve.

The discussions about cybersecurity and the cloud highlight two enduring, often interconnected risk and compliance priorities: *operational resilience* and *third-party risk management*. Operational resilience, which has been an area of focus for the Bank of England, the U.S. prudential regulators and the Basel Committee for several years now, continues to gain steam in other jurisdictions. Global financial institutions, with the assistance of their compliance departments, will need to monitor closely host country developments and any different national approaches that may affect an institution's resiliency program. Regulatory expectations for third-party risk management, which extend well beyond information security requirements, also continue to develop. For banking organisations operating in the United States, as just one example, 2022 should see a rule proposed in July 2021 entitled *Proposed Interagency Guidance on Third-Party Relationships: Risk Management* finalised. This will require commensurate enhancements by banking organisations, as required, to their third-party risk management policies and procedures.

Cryptocurrency: The title of an article published by a business professor in the *Harvard Gazette* in September 2021 succinctly sums up the compliance challenges related to crypto: "Regulators put cryptocurrency in crosshairs." Is crypto the future of banking? Is it the medium of choice for criminals? Is it – can it be – both? What is clear is that regulators are interested in the development of the cryptocurrency market and we can expect more regulation. This will likely include expansion or modification of regulatory regimes to make clear where the responsibility for regulation and supervisory oversight of crypto assets lie as well as determinations that certain classes of crypto assets are securities and will be regulated as such. As financial institution product teams look to satisfy customer demands even as early naysayers are jumping on the cryptocurrency bandwagon, they will need to partner with their compliance departments to understand and respond to applicable regulations and related expectations.

Traditional compliance issues

The priority traditional compliance issues include four persistent challenges, though one has been reshaped by innovation. Each of these four, however, has a nexus to at least one, if not more, of the risk issues discussed above.

Culture and conduct: Culture and conduct have remained in the spotlight for the financial services industry since the 2007-2009 global financial crisis and are continually fuelled by what seem like never-ending financial penalties tied to financial institution misbehaviour. Now, culture and conduct also permeate ESG discussions. While regulatory requirements in some jurisdictions (e.g., the U.K. Senior Managers' Regime and Australia's Banking Executive Accountability Regime [BEAR]) clearly establish some culture and conduct protocols, for the most part, culture and conduct expectations are not prescriptive and the industry continues to

struggle with developing an effective framework that is based on principles and not rules. This already-difficult challenge may become even more imposing in the post-pandemic era, where the likelihood of a hybrid work environment for at least the foreseeable future will make it more difficult to instil and monitor consistent company culture and values.

Vulnerable customers: Vulnerable customers have been defined by the U.K.'s Financial Conduct Authority as customers who, due to their personal circumstances, are especially susceptible to harm – particularly when a firm is not acting with appropriate levels of care. This concept is also a component of the U.S. Consumer Financial Protection Bureau's standards for "unfair, deceptive, and abusive" acts and practices. The notion of vulnerable customers, therefore, is universal, and vulnerable customers have been much on the minds of global regulators since the start of the global pandemic. Because many of these individuals have been disproportionately impacted by the well-documented "K-shaped" economic recovery from the pandemic, regulatory attention is likely to continue. How a financial institution interacts with vulnerable customers also reflects its culture and conduct and, thus, its commitment to ESG.

Areas of regulatory attention may differ somewhat based on where a financial institution conducts business but are likely to include identification and understanding of risk factors, access to credit and credit decisioning, appropriateness of products offered, growth in non-traditional credit products (such as buy now, pay later), clarity and accuracy of customer disclosures, nature of customer engagement and communication, and credit collection practices. Institutions that rely heavily on fee income in categories such as retail deposit overdrafts are also under scrutiny. Compliance departments need to play a continuing role in ensuring that financial institutions have taken the right steps to identify their vulnerable customers; have developed and trained front line personnel on vulnerable customer policies and procedures; and are adhering to these policies and procedures, including redressing promptly and appropriately any deviations from policy and procedures that may cause harm to vulnerable customers.

Use of AI in decision-making: While financial institutions are exploring and adopting artificial intelligence (AI) to assist with a range of tasks, the use of AI in the lending process is particularly in the spotlight. Lenders have long been required to adhere to laws and regulations that prohibit discrimination in their lending decisions. Historically, consumer lending decisions have been made by a loan officer manually on a case-by-case basis. More recently, these decisions have been made by automated credit scoring systems judgmentally designed by humans. Now, increasingly, lenders are looking to AI to make these decisions, tipping the balance in favour of technology over humans. As with so many other areas of innovation, using AI to make lending decisions brings both promise and risk. The promise is that financial institutions will make better-informed risk decisions. The risk is that prior discriminatory practices and even data limitations that may disproportionately impact certain segments of the market will be perpetuated, and even amplified, by AI algorithms. As a result, financial institutions' design and adoption of AI is receiving considerable attention from regulators. Compliance departments should routinely be conducting reviews of AI lending decisions for indications of unintended

bias, which should include ensuring that users of AI models understand the models and their attendant risks and can explain how they work, and collaborating with model risk experts to evaluate and ensure that the variables used in the models and algorithms do not promote bias.

Financial crimes: Whether we trace the origins of financial crime compliance to the publication of the original Financial Action Task Force's 40 Recommendations in 1989 or to specific national efforts such as the enactment of the U.S. Bank Secrecy Act in 1970, one truth applies: No body of financial law and regulation has undergone or continues to undergo more change than financial crimes compliance. Given the global footprint of so many financial institutions, regulatory changes pertaining to financial crimes compliance in any major jurisdiction are likely to have far-reaching implications. In 2022, financial institutions can look forward to additional rulemaking implementing the U.S. Anti-Money Laundering Act of 2020, as well as a package of EU proposals covering a wide range of issues, including enhancing and ensuring the consistency of supervision, strengthening beneficial ownership standards, and strengthening oversight of cryptocurrency. Even if the U.S. and EU regulatory initiatives were the only ones to consider in the coming year – and that is certainly not the case – financial institutions would still be stressed to manage these changes effectively while not losing focus on their business-as-usual responsibilities and the emerging risks that threaten the effectiveness of their financial crimes compliance programs.

Impacts on the compliance department

Compliance departments continue to be impacted by external and internal developments.

Data-led supervision: For a long time, regulators have used peer analyses to shape their supervisory approach. Regulators have become better and better at harnessing and analysing reams of data and using this data more effectively to target their supervisory actions, thus financial institutions will need to pay closer attention to what the data they provide may be telling the regulators. This is particularly true given the regulators' advantage of being able to look across the industry and identify potential outliers or anomalies, e.g., in customer complaints, suspicious activity reporting, or compliance department headcount versus institution size. While compliance personnel are not the only ones in a financial institution providing information to the regulators, the compliance team's interpretations of the regulatory sensitivity of the information provided is likely to take on added importance. And, like the regulators, compliance departments will likely realise that they need to improve their data analysis capabilities (see the people agenda section below) to make sense of the data.

Innovation/cost reduction: For compliance departments, innovation and cost reduction are two sides of the same coin. Although cost-cutting initiatives may have been sidelined briefly as compliance departments, along with all other financial institution functions, transitioned to remote operations during the pandemic, compliance departments are now routinely being asked how they can do more with less even as they continue to launch new products and deal with new regulatory requirements, how they can better leverage technology for everything from providing advice to monitoring compliance, and how they can employ more innovation to reduce headcount and enable their compliance subject-matter experts to focus on where they can provide the greatest value. Technology has been used to support compliance efforts for decades and the opportunities to introduce additional technological innovation seem limitless. Already, we can point to examples of robotic process automation, process mining, data visualisation, AI and machine learning, natural language processing, and more being used in some areas of compliance, with significant opportunity for broader application. In some markets, regulators actively encourage innovation in compliance; in other markets, the regulators are more sceptical and will need to be convinced that innovation improves not only efficiency but also effectiveness. To achieve the benefits of innovation takes time and effort, often meaning that new and old approaches need to run parallel until such time that effectiveness can be proven. In the short term, innovation will further stress already-extended compliance functions.

The people agenda: Many of today's compliance practitioners might not recognise the financial institution compliance department of 25 years ago, when the primary experience necessary to be a successful compliance officer hinged on the technical knowledge of laws and regulations and good communication skills. That's because today, the minimum skills for success include so much more: business judgment and strategic thinking; relationship building and negotiation skills; risk assessment and risk management capabilities across a growing spectrum of risks; data analytics and problem-solving skills; technology savviness; program and project management skills; and an executive presence. Many of these skills are the very same ones being demanded in other areas of financial services and, indeed, in many other industry sectors, as well. Therefore, like it or not, compliance functions are combatants in a highly competitive war for talent and need to go on the offensive to attract and retain the calibre of individuals needed to be successful. This means not only offering competitive benefits and being able to articulate the career potential in compliance, but also expanding the area of recruitment, in terms of both geography and prior experience. It also means focusing on the employee experience by, among other considerations, offering the workplace flexibility available in other organisations in which employees can set their own hours and work from anywhere, and demonstrating to candidates that the organisation is committed to being a leader in innovation and providing the training that will help employees be successful in the digital world.

In closing

Are there other priorities we could have included, such as the changing regulatory landscape in some jurisdictions (including the United States) and the challenges faced by financial institutions trying to compete with new, less-regulated market entrants? Yes, we could have included these and so many more, but we think our list of 13 presents a good starting point in helping position the compliance function for success in the coming year.

Contacts

Carol Beaumier
Senior Managing Director
carol.beaumier@protiviti.com

Bernadine Reese
Managing Director
bernadine.reese@protiviti.co.uk