Thomson Reuters Institute

10 Global Compliance Concerns for 2023

THOMSON REUTERS®

10 Global compliance concerns for 2023

Compliance professionals are balancing a unique set of obligations in 2023. The current geopolitical climate, environmental demands, economic concerns, and other conditions are shaping responsibilities for the year ahead for all compliance professionals.

While each country and region have their own concerns, many overlap in significant ways. The concerns discussed below are important to all compliance professionals, especially those in the United States, the United Kingdom, the European Union, and the Asia-Pacific region.

Further, regulators are now requiring that much more be done with the same — and in some cases less — compliance budgets. Even with competing obligations, it is important for organizations to consider the global impacts of their business dealings — that, more than anything else, is on the horizon for 2023.

The top 10 obligations below provide an insight into each of the concerns that will be critical for compliance officers to manager in 2023.

1. Environmental, social, and governance (ESG) issues

ESG is an important issue across the world and each nation has its own regulatory approach. The cost of doing business must include the cost complying with regulations in jurisdictions where business is conducted.

In the U.S., ESG initiatives are at a critical juncture as they enter 2023, with new rules and regulations emerging across federal and state jurisdictions. Whether policymakers, regulators, and ESG supporters can hold firm and proceed with an aggressive ESG agenda is now uncertain as a partisan divide has intensified in the United States. Several states moved to pull state-managed pension assets from funds that were adopting ESG initiatives while others have proposed legislation or brought lawsuits in opposition to ESG-related rules, regulations, or policies. Thomson Reuters' *Special Report: ESG Under Strain* also highlighted an uneven international regulatory landscape surrounding ESG.

Meanwhile, compliance with the International Sustainability Standards Board's work on climate-related disclosures and the Task Force on Climate-Related Financial Disclosures' (TCFD) recommendations is already well-advanced.

The E.U. has adopted a suite of regulations to address climate-related disclosures, including the adoption of the Sustainable Finance Disclosure Regulation, the Corporate Sustainability Reporting Directive, and Taxonomy regulation.

In the U.K., existing legislation such as the Companies Act has been amended to reflect the TCFD's disclosure requirements. And the Financial Conduct Authority (FCA), the U.K.'s main regulatory body, continues to oversee listed companies' compliance with the TCFD recommendations and requires them to explain any non-compliance.

The Asia-Pacific region has outpaced the United States in terms of sustainable investing and is fast catching up with Europe. Asian regulators have implemented climate risk management policies, and in turn, they expect firms to have dedicated resources and risk management frameworks. Regulators are particularly determined to tackle greenwashing — misrepresenting the extent to which a financial product or investment strategy is environmentally friendly, sustainable, or ethical — following recent customer protection actions.

Around the world, regulators and standard-setting bodies will continue to work with the private sector this year to achieve transparency and consistency of ESG metrics, methodologies, and taxonomies to ensure both efficiency and market integrity.

2. Regulatory change and demands on compliance

In December, the U.S. Securities and Exchange Commission (SEC) proposed a four-part rules-package to set the stage for a significant structural overhaul of the way securities are traded. The new rules would amount to some of the biggest changes in U.S. equity market structure in nearly two decades. Such significant changes would directly affect compliance departments as policies, procedures, technology, and disclosures would need to be adapted.

The package consists of: Regulation Best Execution, Requirements to enhance order competition, Revisions to Regulation National Market System (NMS) and Updated disclosure requirements under Rule 605 of Regulation NMS.

Industry trade groups, such as the Securities Industry and Financial Markets Association have urged caution over the proposal, warning of possible "unintended consequences" to investors.

There have only been a handful of actions thus far directly citing Regulation Best Interest (BI), which went into effect in 2020. However, an enforcement case in 2022 involving the sale of high-risk bonds, and new attention to the rule by the brokerage industry self-regulator, the Financial Industry Regulatory Authority (FINRA), point to the growing importance of Reg BI. (FINRA included Reg BI in its annual exam priorities report, devoting an entire section to it.)

Indeed, Reg BI could become a "catch-all" violation in enforcement actions involving retail investor protection. Therefore, compliance departments should be mindful of its growing importance.

Compliance departments in the E.U. face a different, but equally complex set of obligations. Through the Edinburgh Reforms, the U.K. government has set out an ambitious set of measures to move the U.K. away from the E.U. rules. Most of the reforms are still under consultation, and many of those that have been released to date have targets during the first quarter of 2023. The platform for these changes is the Future Regulatory Framework review; and legislation, in the form of the Financial Services and Markets Bill, is nearing completion through Parliament.

The European Supervisory Authorities (ESAs) — three regulatory agencies established by the E.U. to help facilitate the development and convergence of financial services regulation and supervision across the region — meanwhile, have all issued their work priorities for 2023, including a continued focus on financial stability and the implementation of the Basel III reforms, as well as continuing work to review the regulations on packaged retail investment and insurance products (PRIIPs), further guidance on the implementation of cross-sectional areas of the Securitization Regulation and other areas such as ESG, operational resilience, and the ongoing impact of Brexit.

3. Global political tensions and sanctions

Russia's invasion of Ukraine sparked an unprecedented round of sanctions which caused anti-money laundering (AML) and know you customer (KYC) compliance professionals and sanctions departments to go into overdrive to comply. Even non-financial services firms were affected in unanticipated ways, and the importance of ultimate beneficial ownership has become a global legal and regulatory challenge.

With the war still raging and escalated tensions between China and Taiwan also a concern, geopolitical uncertainties will keep compliance and legal professionals on edge regarding sanctions compliance.

Despite advances in legal, regulatory, and sanctions compliance processes, the sheer amount of work involved remains burdensome for many firms, which every day must record their time spent reviewing accounts, companies, and individuals in relation to suspect transactions connected to Russian businesses, individuals, or organizations. There could also be potential reputational repercussions for those firms which get sanctions compliance wrong.

Compliance teams also need to prepare for the possibility of a polarizing split within the international financial system over the continued implementation of sanctions and doing business with Russia.

4. Anti-money laundering and financial crimes

Compliance officers will need to keep financial crime on their radars during 2023, and that can cover a wide range of areas. For example, the regulatory focus on anti-money laundering (AML) resulted in total fines during 2020 and 2021 of around £476 million in the U.K. alone, including penalties imposed against such high-profile financial service firms as NatWest, HSBC, and Credit Suisse. Further, there have been enforcement actions for market abuse during 2022, and fraud is predicted to increase in 2023.

The U.K. Economic Crime Bill, which is progressing through Parliament, seeks to deliver reforms to make it easier to act where economic crime is perpetrated. And the German regulator, BaFin, ordered Deutsche Bank to take specific measures aimed at preventing money laundering and terrorist financing; while in the U.S., the long-running fraud scandal at Danske Bank resulted in the bank pleading guilty to fraud conspiracy and agreeing to forfeit $2 billion.

5. Proliferation financing

Similarly, financial services firms may also find themselves having to address the risk of *proliferation financing*, which occurs when an entity makes available an asset, provides a financial service, or conducts a financial transaction to facilitate the proliferation of weapons of mass destruction, regardless of whether the activity occurs or is simply attempted.

Other significant threats in this area include the use of third-country nationals to facilitate proliferation financing and evade sanctions through trusts, and shell companies using alternate directors or false identification to circumvent sanctions or restrictions.

This is especially significant for compliance teams now because the conflict in Ukraine has intensified pressure on sanctions compliance and increased the enforcement risk over lapses or sanctions evasion.

6. Digital assets & cryptocurrency

It's not surprising that the hot-button issues of digital assets and cryptocurrency are something to which compliance officers will have to pay special attention in the coming year.

E.U. policymakers agreed on the text of the Markets in Crypto-Assets (MiCA) regulation in mid-2022, and once passed, the regulation will provide a comprehensive set of measures to protect consumers by ensuring the safety and soundness of crypto

services. MiCA is due for passage through Parliament in early 2023, and its provisions will come into effect across mid-to-late 2024. MiCA's comprehensiveness means that it will become the blueprint for crypto-regulation in other jurisdictions during 2023, as regulators everywhere work to prevent more chaos, such as the collapse of the FTX crypto exchange.

In 2023, the U.S. faces a race to catch up with its international counterparts in regulating digital assets. The urgency comes on the heels of the tumultuous 2022, in which the digital asset sector lost more than $2 trillion in market value, sinking below $1 trillion. In addition to asset-price declines, the implosions of crypto firms such as FTX, Celsius Network, and Terra Luna and allegations of fraud have fueled public and political pressure on U.S. regulators and policymakers to act.

Regulatory priorities are likely to be focused on ensuring financial stability, consumer protection, and combating fraud and illicit activity. The activities regulators and lawmakers are likely to target include stablecoins — asset-backed cryptocurrencies — and centralized exchanges.

In 2022, Thomson Reuters Regulatory Intelligence published a *Special Report: Cryptos on the rise*, covering the emerging market's complex global regulatory future. Amid the industry turmoil and headline-grabbing criminal investigations, compliance and legal professionals must stay abreast of the regulatory developments while exercising caution before wading into the uncertain waters of digital assets.

Another indirect result of the FTX collapse is the closer regulatory scrutiny of private equity (PE) firms, including their due diligence procedures and valuation practices. The SEC is said to be seeking details about the due diligence performed by PE firms and their investments in FTX.

In Asia, the Singapore government's attitude toward digital assets and blockchain technology, for example, has remained largely unchanged. "We encourage and support innovation in digital assets because we see potential for new technologies to transform cross-border payments, trade and settlement, as well as capital market activities," said Lawrence Wong, deputy prime minister and minister for finance.

Central bank digital currencies (CBDCs) are being researched by governments around the world and, if rolled out, could revolutionize the financial system and even replace physical cash. No advanced economy has yet committed to issuing a general-purpose CBDC, but Australia, China, Hong Kong, and Singapore have carried out extensive research, and the Monetary Authority of Singapore introduced a pilot scheme in 2022.

7. Increased focus on accounting

Private equity issues, particularly the recent suspension of redemptions with the $69 billion unlisted Blackstone Real Estate Investment Trust, raise questions surrounding valuations of the underlying assets held in PE funds. If liquidity is problematic, the logical next question is often related to whether the assets are properly valued. If valuations are incorrect, the problems cascade pertaining to issues such as fees charged to investors.

Accounting practices such as the use of independent external auditors — also a central theme in the crypto failures, and an ongoing battle related to accounting by Chinese companies listed in the United States — have raised the importance of accounting and auditors with regulators.

In the U.S., the Public Company Accounting Oversight Board (PCAOB) and its chair, Erica Williams, are poised to take a more prominent role and step-up enforcement activities. Williams has been bringing cases citing previously unused provisions, including violations that resulted from negligent conduct such as failure to supervise — and some penalties have been steep.

These actions came amid criticism that PCAOB had been too lenient towards auditors and needed to pay more attention to its stated mission of protecting investors, something Williams disputes. "The PCAOB is serious when it comes to enforcement," Williams said in December.

In 2023 senior management, compliance professionals, and legal departments should raise the overall importance of accounting-related compliance.

8. Data governance & protection

Data governance is relevant for compliance officers on several levels. At the jurisdiction level, for example, many countries have data strategies in place — both the European Commission and the U.K. government have published high-level visions that outline how a data framework would work.

Regulators also are keen to explore ways to maximize the use of regulatory data. The U.K.'s FCA provided a progress report on its data strategy in 2022, including actions to be undertaken from 2023 and beyond. And the work program for the European Banking Authority (EBA) for 2023 prioritizes measures to "enable the EBA to share data and insights with internal stakeholders and the whole data ecosystem." Finally, the European Securities and Markets Authority has included "facilitating technological innovation and effective use of data" as one of its strategic priorities for the next five years.

Data governance also has relevance at firm level, because firms must embed a framework which encompasses all aspects of data governance, from creation to destruction of corporate, governance, and customer data. The greater emphasis upon which regulators are placing the amount and quality of data to be reported places pressure on firms to be able to deliver that data. This is an area where firms often have proven to be weak. In one recent example, Sigma Broking Ltd was fined £500,000 for market abuse and transaction-reporting failures.

On a related front, the war in Ukraine has seen a growth in cyber-warfare and the attendant risks. In a trend which has been described as "profound and new", criminal gangs and hostile nation states are working together to destroy or compromise commercial interests. They aim to exploit critical infrastructure vulnerabilities, scanning technology networks with "unpatched systems" to identify weakness within large corporations and potentially cripple them.

The cyber-attacks have set off destructive malware which not only resulted in significant damage in Ukraine itself but also caused widespread damage to international networks. Australia, for example, has experienced a marked increase in ransomware attacks as both telecommunications firm Optus and health insurer Medibank Private were both targeted by attackers who stole the sensitive information of millions of individuals and then attempted to blackmail the firms in return for not releasing the stolen data onto the internet. Medibank Private refused to pay the ransom to a suspected Russian organized crime syndicate, while many experts disagree on whether ransoms should be paid in such circumstances.

Such attacks look set to proliferate in 2023. Senior managers at both Optus and Medicare Private thought they had sufficiently strong cyber-resilience systems in place at the time of the attacks, but they were proved wrong. Firms would be well-advised to improve their data management governance in the year to come.

9. Technology, cybersecurity and artificial intelligence (AI)

Digitalization and the use of technology has spread widely in recent years, and the fintech and regtech sectors have grown dramatically. Thomson Reuters Regulatory Intelligence's *Fintech, Regtech and the Role of Compliance in 2023* survey reported signs of a slowdown in the growth of the fintech sector, finding that while international growth in the first half of 2022 had plateaued, the U.K. fintech marketplace had continued to grow.

Fintech applications have continued to be used in diverse ways, from payment systems to know-your-customer verification, to robo-advice and claims handling. Technology is

also used to facilitate the hybrid working arrangements which proliferated during the pandemic — for example, the use of fintech applications to monitor communications.

In its annual risk report, the EBA highlighted an increase in the use of artificial intelligence (AI) solutions. Eighty-three percent of respondents to the EBA's survey reported that they already use AI, and an additional 12% are either pilot-testing or developing AI systems.

Financial services firms' ability to deploy and maintain these applications is being tested, and they are increasingly relying on third-party providers that have the expert knowledge and technical resources to be able to manage such systems. The likelihood that Big Tech will begin to play more of a part in financial services also presents risks, however. The Bank for International Settlements explored this topic in a paper, *Big Tech regulation: In search of a new framework*.

Compliance officers may therefore need to shift their focus in 2023 from managing internal digital deployment to managing the risks associated with outsourcing such development to third-party service providers.

Indeed, regulators have already begun to address these concerns. The Prudential Regulation Authority (PRA) issued a supervisory statement in March 2021 setting out its expectations for how PRA-regulated firms should comply with regulatory requirements related to outsourcing and third-party risk management to improve business resilience. This was followed up in the middle of last year by a joint-discussion paper from the PRA, the FCA, and the Bank of England on how to deal with third parties critical to the U.K. financial sector.

In the E.U., the ESA responded to the European Commission's February 2021 call for advice on digital finance and related issues by making recommendations concerning third parties.

10. Human capital

As compliance officers' responsibilities expand, so too does the range of expertise and knowledge they need to optimize their skill sets. The availability of relevant skills, or the lack thereof, has featured heavily in Regulatory Intelligence's *Cost of Compliance* surveys in the last few years. For example, of the 66% of respondents to the 2022 survey who said they expected the cost of senior compliance staff to increase, nearly half (47%) cited the demand for skilled staff and knowledge as the top reason. This correlates to increasing demand for compliance expertise in areas such as ESG, digitalization and technology, as well as other niche areas.

Following the pandemic, the job market for compliance professionals improved in 2021, particularly for such disciplines such as AML and fintech. More recently, however, there have been indications that demand for more senior compliance roles has waned, with a greater need to fill junior or mid-level roles.

While this appears to reflect firms' reaction to the economic situation, many compliance departments nevertheless continue to lack the required level of expertise needed.

Overall, this year also will undoubtedly see the need for compliance officers to have at least one eye on the regulatory perimeter — along with many of the other areas discussed above. With regulators working on new areas such as non-bank financial intermediation, buy now/pay later products, and crypto-assets, it will be essential for compliance officers to remain vigilant about developments that expand the jurisdiction of financial regulators and require more of their compliance time.

Credits

Thomson Reuters Regulatory Intelligence

Reporters: Todd Ehret in New York, NY
Niall Coburn in Brisbane, Australia
Mike Cowan in London, United Kingdom

Editors: Alexander Robson in London
Randall Mikkelsen in Boston, MA

Thomson Reuters Institute

Editors: Rabihah Butler in Charlotte, NC
Gregg Wirth in Bloomsburg, PA

Thomson Reuters

Thomson Reuters is a leading provider of business information services. Our products include highly specialized information-enabled software and tools for legal, tax, accounting and compliance professionals combined with the world's most global news service – Reuters.

For more information on Thomson Reuters, visit **tr.com** and for the latest world news, **reuters.com**.

Thomson Reuters Institute

The Thomson Reuters Institute brings together people from across the legal, corporate, tax & accounting and government communities to ignite conversation and debate, make sense of the latest events and trends and provide essential guidance on the opportunities and challenges facing their world today. As the dedicated thought leadership arm of Thomson Reuters, our content spans blog commentaries, industry-leading data sets, informed analyses, interviews with industry leaders, videos, podcasts and world-class events that deliver keen insight into a dynamic business landscape.

Visit **thomsonreuters.com/institute** for more details.

THOMSON REUTERS®