10 Things compliance officers need to consider in 2022

THOMSON REUTERS®

Ten things compliance officers need to consider in 2022

Heading into 2022, the pandemic should have been in the rear-view mirror, but instead the world is dealing with the impact of another variant of COVID-19. One lesson financial services firms and their compliance officers have learned is the importance of operational resilience. Many firms had scheduled post-pandemic reviews but those have morphed into a rolling review of the efficacy of hybrid-working arrangements.

Policymakers and regulators alike are focused on operational resilience. This is defined as the ability of firms, financial market infrastructures and the financial sector as a whole to prevent, adapt and respond to, recover and learn from, operational disruption. Specifically, an operationally resilient financial system is one that can absorb shocks rather than compound them.

The need for operational resilience encompasses every activity a firm undertakes and is even more critical for any activity carried out by a third party. The continuing disruption caused by the pandemic has highlighted just how critical it is for firms to know who they are dealing with and to map exactly what is happening, and where. They must also ensure that it is monitored, assessed and included in their compliance and risk reporting.

Risk and compliance officers will play a central role in preparing their firms for all eventualities. The following is a list of things they need to consider in 2022.

Susannah Hammond
Senior Regulatory Intelligence Expert
Thomson Reuters Regulatory Intelligence

1 Shifting individual accountability

The concept of personal liability for senior managers in financial services firms is not new. What is new is the changing perception of the potential sources of liability and how regulators are interpreting accountability. Accountability and enhanced corporate governance regimes are proliferating worldwide, and senior managers now need to consider an increasingly wide range of non-financial misconduct when assessing whether individuals are deemed to be fit and proper to undertake financial services.

Firms are wary of the potential for reputational and other damage, and this has implications for individuals — even those at the most senior levels. Examples of non-financial misconduct have included everything from stealing sandwiches to failing to pay for train tickets to manipulating college admissions. In one high-profile case, Jes Staley, the chief executive of Barclays, stepped down due — at least in part — to concerns about his connection with sexual offender Jeffrey Epstein.

The rise in the number of non-financial misconduct cases has taken place alongside more mainstream enforcement actions. Just one example is the action taken by the Dubai Financial Services Authority against senior individuals at the former Abraaj Group. The chief financial officer was banned and fined $1.7 million, and the managing partner was banned and fined $1.9 million. Both were involved in carrying out unauthorised financial service activities and actively misleading investors in Abraaj funds.

For compliance officers, it is a double whammy; not only do they have to help their firm navigate the shifting expectations of fit and proper and compliance breaches but they themselves, on a personal basis, need to be wary of the widening scope of potential personal liability.

The matter was the subject of a proposal by the New York City Bar Association, which recommended a framework for senior compliance officer liability to seek to address the "sustained tide of concern" arising from enforcement actions holding chief compliance officers personally liable, in particular for actions that did not stem from fraud or obstruction on their part.

The wider challenge is that career-ending enforcement actions can potentially discourage individuals from becoming or remaining compliance officers and performing vital functions that regulators, stretched too thin, would otherwise be unable to undertake. This is particularly the case when other options, such as providing legal advice or becoming an outside compliance service provider or businessperson, involve less personal risk.

2

Vulnerable customers

Compliance officers have long been aware of the need to ensure consistently good customer outcomes. A vulnerable customer is someone who, due to their personal circumstances, is especially susceptible to harm. All customers are at risk of becoming vulnerable, but this risk is increased by having characteristics of vulnerability.

Previously, these characteristics have included: poor health, such as cognitive impairment; life events, such as new caring responsibilities; low resilience in terms of coping with financial or emotional shocks; and low capability, such as poor literacy or numeracy skills.

Firms now need to add to the list of vulnerability characteristics the possible impact of digital transformation. Many financial services firms have leveraged digital transformation and deployed enabling technologies in response to the pandemic, but vulnerable customers risk being left behind by technological change — particularly when that change has happened at speed.

Not all customers who have vulnerable characteristics will experience harm. They may, however, be more likely to have additional or different needs which, if firms fail to meet them, could limit their ability to make decisions or represent their own interests, putting them at greater risk of harm. Compliance officers therefore need to develop appropriate policies and procedures to ensure an appropriate level of care for potentially vulnerable consumers.

3

Personal account dealing

Hybrid or non-office working environments have prompted a regulatory focus on the potential for market abuse and manipulation. That focus needs to extend to personal account dealing.

The issues occurred pre-pandemic, but the impact and implications of a personal account dealing fine imposed by the Central Bank of Ireland (CBI) should be taken as a warning to all. In March 2021, the CBI reprimanded J&E Davy and fined it 4,130,000 euros for regulatory breaches arising from personal account dealing whereby a group of 16 Davy employees dealt in a personal capacity with a client.

Davy was Ireland's largest stockbroker and wealth manager, with approximately 48,000 active clients and 8.5 billion euros assets under management. The CBI found that Davy prioritised facilitating an opportunity for personal financial gain over ensuring that it was complying with its regulatory obligations. The CBI determined the appropriate fine to be 5,900,000 euros, which was reduced by 30% to 4,130,000 euros in accordance with the settlement discount scheme.

Specifically, Davy lacked a control framework to prevent employees from executing personal transactions that could give rise to a conflict of interest. The senior employees concerned circumvented the personal account dealing framework completely, such that Davy's compliance function first became aware of the transaction four months later, when certain information became public.

The fallout from the personal account dealing failings has been profound. The chief executive stepped down, and Davy lost its role as primary dealer in Irish government debt and has now been sold.

4 Cyber resilience

Information and cyber-security risks have increased during the pandemic, with the financial sector reported to have been hit more often by cyber-attacks than most other sectors since the pandemic started. As just one example, data on attacks has highlighted a strong link between the prevalence of working-from-home arrangements and the incidence of cyber-attacks between the end of February and June 2020. Payment firms, insurers and credit unions are seen to have been especially affected.

The financial sector was already a target of cyber-attacks before the pandemic. Companies of all sizes are vulnerable to attack in the online world. In terms of information security, cyber resilience, cyber risk and cyber crime, as well as cyber-attacks, both operational resilience and good customer outcomes will be under threat in the event of a failure of cyber hygiene.

Christine Lagarde, chair of the European Central Bank (ECB), told a Reuters Newsmaker in April 2021 that the greatest economic threat is that of cyber. This was echoed by Wayne Byres, chair of the Australian Prudential Regulation Authority (APRA), in a speech to the Committee for the Economic Development of Australia.

"Of the three areas I've covered, cyber presents arguably the most difficult prudential threat: unlike GCRA [governance, culture, remuneration and accountability] or climate risk, it's driven by malicious and adaptive adversaries who are intent on causing damage. Cyclones and bush fires can be devastating, but they're not doing it on purpose," Byres said.

Information and cyber security have always posed regulatory risks, but the pandemic and associated digital transformation have amplified the threat. Firms and their compliance officers remain on notice about the need to identify, manage and, whenever feasible, offset cyber and information security risks.

Specifically, risk and compliance functions need to ensure that information security and cyber risks are included in the range of risks considered, and that the board can discuss the actions taken to ensure all reasonable steps have been taken to embed cyber resilience throughout the firm.

Firms may need to invest in specific technological skills to ensure their boards can meet growing regulatory expectations in terms of information security and cyber risk management.

5 Diversity

Diversity has climbed up the regulatory agenda as it has come under the umbrella of environmental, social and governance (ESG) concerns — which are fast becoming a strategic priority for firms and regulators alike. Alongside the need to tackle climate change, questions about human rights, social justice and human diversity now also need to be managed alongside firms' more traditional values and concerns.

Investment managers, banks, securities firms and their regulators face a difficult task because the risks associated with ESG are often so new that they are difficult to quantify. There is an understandable urgency about climate risk, but firms are also striving to address a slew of additional social problems, one of the most important of which is diversity.

The lack of international policy harmonisation means firms often find themselves dealing with inconsistent policies and disclosure requirements. How well, or otherwise, they deal with navigating the divergent rules and regulations will depend on their governance, compliance, human resources and risk management processes.

Compliance officers need to assess whether their firm has a comprehensive approach to diversity and whether it is able to embed the new risks within the existing enterprise risk frameworks. They also need to delineate the specific roles and responsibilities for the compliance, human resources and risk management functions, and assess whether those functions have the right talent with the required skill sets.

6

Hybrid working

Hybrid working is here to stay. Compliance functions have adapted to hybrid, or at least flexible, working arrangements but may need deal with further changes as the pandemic continues.

The UK Financial Conduct Authority's (FCA) October 2021 codification of its previous expectations regarding firms' hybrid working arrangements provides a useful risk management checklist. The FCA said firms must be able to prove there is satisfactory planning, such that:

- There is a plan in place, which has been reviewed before making any temporary arrangements permanent and that it is reviewed periodically to identify new risks.
- There is appropriate governance and oversight by senior managers under the senior managers regime, and committees such as the board, and by non-executive directors where applicable, and that this governance is capable of being maintained.
- A firm can cascade policies and procedures to reduce any potential for financial crime arising from its working arrangements.
- An appropriate culture can be put in place and maintained in a remote working environment.
- Control functions such as risk, compliance and internal audit can carry out their functions unaffected, such as when listening to client calls or reviewing files.
- The nature, scale and complexity of its activities, or legislation, does not require the presence of an office location.
- It has the systems and controls, including the necessary IT functionality, to support the above factors being in place, and these systems are effective.
- It has considered any data, cyber and security risks, particularly as staff may transport confidential material and laptops more frequently in a hybrid arrangement.
- It has appropriate recordkeeping procedures in place.
- It can meet and continue to meet any specific regulatory requirements, such as call recordings, order and trade surveillance, and consumers being able to access services.
- The firm has considered the effect on staff, including wellbeing, training and diversity and inclusion matters.
- Where any staff will be working from abroad, the firm has considered the operational and legal risks.

"The above is an indicative and non-exhaustive list. It's important any form of remote or hybrid working adopted should not risk or compromise the firm's ability to follow all rules, regulatory standards and obligations, or lead to a failure to meet them," the FCA said.

7

Climate risk reporting

Climate risk is unlike other financial risks. Its uniqueness and complexity, and the long-term nature of the risks, make quantifying the threat one of the biggest hurdles regulators must overcome in developing new rules and regulations. One success at COP26 was the agreement on standards and financial services. Firms and their compliance officers need to engage to ensure that "good", internationally coherent, regulations continue to be developed.

Specifically, firms need to consider the ramifications of the general requirements for disclosure of sustainability-related financial information prototype.

The objective of the standards is to require entities to provide material information about the entity's exposure to sustainability-related risks and opportunities that will help users of general-purpose financial reporting to make decisions about whether to provide economic resources to the entity. The standards also seek to enhance connectivity within the entity's general purpose financial reporting, including between the entity's financial statements and sustainability-related financial information.

The International Sustainability Standards Board disclosure standards, while still technically "draft", will become the international reporting benchmark on sustainability matters.

To that end, and to meet users' needs, firms will be required to report material information on sustainability risks and opportunities, which would assist users in predicting the value, timing and certainty of the entity's future cash flows in the short, medium and long term, and therefore their assessment of enterprise value.

To the extent it could influence the assessment of enterprise value, material information includes information about the entity's impacts on society and the environment, and how those impacts affect its future cash flows. Comparable disclosure on sustainability matters relevant to assessing enterprise value is designed to help facilitate the efficient allocation of capital.

Firms will have to be able to regularly collect, collate, manage and reproducibly report millions of data points. To do so, they will need to ensure that the lessons of past wholesale reporting failures (transaction reporting in the wake of the implementation of the Markets in Financial Instruments Directive being a case in point) have been learnt.

Post-COP26, firms simply cannot allow another widespread failure to deliver on new reporting obligations. Fines and remedial actions likely to be severe, and there is also the spectre of greater personal liability and reputational damage if a firm is seen not to have taken its climate risk obligations seriously.

The Regulatory Intelligence special report on the fast-moving challenges for firms arising from ESG can be downloaded here.

8

Digital transformation and cryptos

Digital transformation will continue to be a fundamental enabler for financial services firms. The opportunities and benefits arising from the implementation of technological solutions cannot be underestimated, but taking best advantage of those opportunities is not without its challenges.

Cryptos have emerged into the mainstream. The deployment of crypto-assets has great potential to make payments and transfers more efficient. The speed and reach of transactions, however, together with the potential for anonymous activity and for transactions without financial intermediaries, also make crypto-assets vulnerable to misuse and raise the risk of money laundering. Policymakers, regulators and firms all need to play their part in ensuring that cryptos are as "safe" as possible, not only in terms of investment risk but also with regards to regulatory certainty and cyber resilience.

In particular, supranational policymakers must continue to work toward consistent definitions of what is, and what is not, inside the regulatory perimeter. Cryptos may be treated as a currency, an investment or a security under current regulatory regimes, or they may not be covered at all.

A good first step would be alignment on definitions. Even if jurisdictions end up banning some or all cryptos (particularly for retail customers), it would be on the basis that international financial services had a common understanding of what was legal, and where.

Compliance functions will need to keep pace with the rapidly evolving regulatory overlay for crypto-assets. Singapore, Bermuda, the EU and the UK are establishing themselves as crypto allies, to varying degrees. Parts of Africa and India have meanwhile taken steps to restrict or prohibit citizens from owning or using cryptos.

A potential game changer could be the formal adoption of central bank digital currencies (CBDCs). None of the G7 countries have, as yet, said they would adopt CBDCs but several jurisdictions are considering the concept and its implications. It is another area where compliance functions and their firms will need to engage to help ensure the development of good regulation.

9

Financial crime

Financial crime remains a perennial concern. Some factors are pandemic-related, with concerns about the rise of cyber-enabled financial crime. An update from the Financial Action Task Force in December 2020 considered changes in behaviour because of the pandemic — whether that of individuals, companies or governments — and which have in turn presented criminals with new, mainly cyber, opportunities to commit crimes and launder the proceeds.

Other factors stem from the shifting geopolitical landscape, to which jurisdictions often respond with targeted but internationally incoherent sanctions. All firms are aware that a sanctions compliance programme is a core competency. A risk-based approach to sanctions monitoring has always been part of a financial services firm's obligations regarding the combatting of financial crime.

Sanctions screening, sanctions compliance and evidencing compliance with the under- and overlapping requirements remains a challenge. A few of the more immediate concerns needing compliance consideration are the approach to Afghanistan following the Taliban takeover, the emerging use of sanctions against a crypto exchange deemed to be a conduit for illicit funds and the implications of the Chinese counter-foreign sanctions law.

10 Skills

The increasingly wide range of challenges coming under the compliance remit all demand appropriate resources and skills. On one level, compliance functions need up-to-date skills, but it is part of the challenge to identify the particular skills, knowledge and experience required for dealing with emerging new risks such as climate, diversity, operational resilience and digital transformation.

The need for up-to-date skills also applies to the board and senior managers, who need to be able to interpret, understand and take appropriate actions informed by the risk and compliance reporting on all aspects of a firm's obligations.

Skills gap analyses need to be undertaken on a regular basis and firms need to be prepared to invest — at all levels — in the skills found to be lacking.

The updating of skill sets has already started. The "Fintech, Regtech and Role of Compliance in 2022" survey report found that 61% of boards have had to widen their skill sets to accommodate developments in innovation and digital disruption regarding fintech (72% for global systemically important financial institutions (G-SIFIs)), while 54% have widened their skill sets for regtech (64% for G-SIFIs).

Firms need to keep an open mind about the skills required and should also be aware that there is likely to be increasing competition for talent as the range of specialist, often technical, skills needed expands.

ABOUT THE AUTHOR

Susannah Hammond is senior regulatory intelligence expert for Thomson Reuters with more than 25 years of wide-ranging compliance, regulatory and risk experience in international and UK financial services. She is co-author of "Conduct and Accountability in Financial Services: A Practical Guide" published by Bloomsbury Professional.
uk.linkedin.com/in/susannahhammond @SannaHamm