10 Things compliance officers need to consider in the Asia-Pacific region this year

THOMSON REUTERS®

INTRODUCTION

Financial regulators in the Asia-Pacific region have shifted from a consultative supervisory stance to a more enforcement-orientated approach, with zero tolerance for any form of misconduct. The near-weekly announcements of large fines and penalties suggest however, there is still progress to be made in terms of improving internal compliance controls, culture and management accountability, and in providing services which are in customers' best interests.

Many of the serious compliance failures seen in the past year did not so much involve a breakdown in systems and controls, but rather a failure on the part of senior management to be direct with customers and level with regulators.

Regulators' new stance on enforcement has been reinforced by the introduction of numerous additional rules and guidelines on accountability, client interest, anti-money laundering/counter terrorism (AML/CFT) financing, data protection, cyber security and digitalisation. Financial institutions are also having to deal with the ever-increasing ambit of financial crime.

Added to this mix is the strain imposed by the continuing pandemic, notably operational resilience considerations, the safety of staff and the retention of specialist in-house skills. In the background are the challenges posed by volatile international markets and the creeping unknown risks hovering around crypto-assets and Stablecoins.

This article sets out the 10 areas which the author predicts will be the main challenges for compliance professionals, firms and regulators during 2022. It provides practical insights to help organisations assess the risks they face.

Niall Coburn

Regulatory Intelligence Expert

1

Shifting regulatory sands

There appears to be no let-up in the volume of supervisory demands placed on firms in the region. Chinese regulators have introduced reforms and taken enforcement action in relation to anti-trust and cyber security and have peeled back the growth of large tech and funds management companies.

The recent move by Hong Kong's primary insurance regulator, the Insurance Authority, to take over a motor insurance firm has proved controversial, forcing firms to come to terms with the likelihood that regulators will take an increasingly determined stance on misconduct. Singapore has stepped up enforcement for money laundering lapses, misinformation to customers and market abuse, and has not hesitated to ban directors who provide false information to regulators.

The Malaysian government, meanwhile, has successfully pursued Goldman Sachs and Deloitte PLT for their involvement in the 1 Malaysia Development Berhad Fund (1MDB) and is casting its net more widely to pursue JPMorgan and Deutsche Bank, both of which were associated with transactions.

The Australian securities regulator has for the first time, taken criminal action against large insurers for mis-selling products, and has levied record-breaking fines on banks for major compliance failures – Westpac Banking Corporation was required to pay more than A$1 billion in fines for AML failures.

Climate change disclosures and digitalisation guidelines may also affect core banking operations and change the way firms do business in the future. For example, rapidly increasing internet access in Asia will lead to an explosion in virtual banking, capturing millions of unbanked clients in Indonesia, Malaysia, Thailand, Vietnam, Philippines and Laos.

Regulators are also considering the introduction of regulatory frameworks for crypto-assets and Stablecoins which may present heightened risks in terms of AML oversight. Some governments are considering whether to introduce their own crypto-assets framework through central bank operations.

1 Shifting regulatory sands

With trading volumes in crypto finance reaching new heights, regulators have yet to agree on a consistent framework and continue to warn the retail market about the increase in crypto-related scams. In the UK, the United States and Europe, regulators are moving to ban social advertising by unlicensed individuals, celebrities and firms.

Despite this regulatory overload, firms are still expected to maintain operational resilience, as well as having to deal with the social and economic impact of the pandemic on staff and business operations. Regulators still expect firms to have systems in place to guarantee the reliable delivery of services and ensure the protection of customers' accounts and assets.

Compliance officers will also have to deal with geopolitical machinations in relation to U.S. sanctions, as well as the health and safety issues associated with employees working from home and employees' freedom to decide whether to be vaccinated.

Compliance professionals should begin by carrying out a holistic review of the immediate risks facing their organisation and then considering how those risks can be offset, and what will make the organisation more resilient in 2022 and beyond.

Tips for compliance professionals

- Attend the organisation's strategic meetings and be involved when significant decisions are made.
- Consider the immediate risks to the organisation (and the business lines) and address each one.
- Understand those issues which, while they affect the organisation, are not strictly in the compliance remit but may have implications for the conditions of, for example, a firm's licence, such as maintaining skill sets in certain areas of the business (despite the shortage of staff).
- Understand the immediate and long-term regulatory expectations relevant to the organisation.
- Ensure there is a clear line of sight in terms of senior management accountability for the different business operations and ensure responsibilities within the organisation are covered.
- Ensure cyber risks are addressed, and customer assets protected.

2

Financial crime

Financial crime remains at the top of the regulatory agenda in the region, with scrutiny focused on banks and insurers. The pandemic and remote working will continue to increase the risk of cyber-crime, underlining the need for operational resilience.

Regulators will focus their enforcement resources on cyber-crime, product mis-selling, market abuse, money laundering, dealing with vulnerable customers, sanctions and corruption. Nearly all the penalties imposed on financial institutions last year followed dishonesty on the part of senior management and/or failure to disclose serious contraventions to regulators.

A particular example in Australia was the "fees for no service" scandal, where firms were found to have collected premiums and fees for services which had not been delivered for at least a decade. It emerged that senior management had been aware of what was happening but took no action. More recently, the Securities Futures Commission ("SFC) reprimanded and fined Citigroup Global Markets Asia Limited US$44.6 million for serious regulatory failures over client facilitation activities. The SFC considered that "such pervasive dishonest behaviour would not have continued but for the serious lapses and deficiencies in its internal controls, compliance function and management oversight."

2

Financial crime

In other cases, senior management appeared blind to "red flags" and allowed misconduct to fester. Even though senior management accountability regimes had been in place since 2018, individual directors were not penalised for these lapses in judgement and honesty (this is discussed in more detail under point 7, management accountability).

The lesson here is that many of last year's cases in the region that came to light still expose a culture within organisations that encourage chasing revenue at the expenses of basic standards of honesty.

Most of the accountability regimes established in the region demand early disclosure to regulators, and failure to do so will attract regulatory penalties. Compliance professionals must hold senior management to account by maintaining effective systems to ensure integrity.

Tips for compliance professionals

- Are customers' interests being protected — bearing in mind recent regulatory action against international firms?
- Does your organisation's culture encourage chasing revenue at the expenses of basic standards of honesty?
- Identify the organisation's threat landscape and offset risks.
- Evaluate the continuing cyber scams that will affect the organisation this year and warn customers.
- Establish whether there are any concerns about mis-selling products to customers, and whether the information provided to customers is accurate.
- Decide whether there is a need to review the use of algorithms and their calculations for customer payments.
- Are material issues being disclosed to regulators?

3

Crypto-assets and uncertainty

2022 will be a landmark year for crypto-assets, as regulators attempt to devise appropriate regulatory frameworks.

Hong Kong and Singapore have already released proposals for crypto-asset regulation, and the Australian Senate has endorsed a crypto-asset framework. Malaysia, the Philippines, Thailand and Japan are also mulling over the development of regulatory frameworks to accommodate the growth of the crypto market, with each jurisdiction vying for their own market share.

China, on the other hand, continues to ban crypto-assets, has restricted the trading of cryptocurrencies and is working toward the development of a central bank digital currency (CBDC). Pakistan is likely to move in the same direction, while India remains "on the fence", but plans to develop a digital rupee to counter China's CBDC.

Regulators are struggling to keep up with innovation, however, and have repeatedly warned investors about the risks. Crypto-assets have not yet posed a material risk to financial stability, but the growing links between crypto-assets and Stablecoins and the traditional financial system make it a threat that regulators cannot ignore.

The main risks are the potential for crypto-assets to be used to launder assets and the inability of central banks and governments to control the flow of multi-dimensional crypto products across borders, leaving regulators unsure how to protect retail investors.

3

Crypto-assets and uncertainty

Another concern is the seeming inability of different jurisdictions to agree on consistent definitions and taxonomies for crypto-assets. Simple questions remain unresolved: What is a "crypto-asset" or "stablecoin"? How will such assets intersect with the traditional financial system? What is the point of acquisition? What is the point of sale or tax? Until regulators settle on a consistent and comprehensive approach, the uncertainty and risk warnings for retail investors will continue.

Traditional financial institutions have already begun to launch crypto-assets, and while take-up has been promising, the absence of a regulatory framework and taxonomy means compliance teams must ensure careful management of the sale of such products. They must be clear about to whom these products are marketed and sold and must ensure warnings and disclosures make the associated risks sufficiently clear to customers.

Tips for compliance professionals

- Ensure crypto-assets are not being sold to retail investors.
- Ensure appropriate disclosure of risks.
- Understand the regulatory approach to crypto-asset products in your jurisdiction.

4

Mis-selling products and quality of advice

Many of the large regulatory fines levied in Australia, Hong Kong and Singapore last year arose from careless marketing of products and non-disclosure to customers. At some firms, senior management failed to monitor conflicts of interest and the sale of products and lacked the back-office procedures to protect customers or ensure adequate disclosure of conflicts of interest.

Regulatory fines for mis-selling products and conflicts of interest have increased exponentially in the last five years, reflecting the seriousness with which regulators and courts view such misconduct.

In Australia, regulatory scrutiny of mis-selling has soared since the 2018 Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry. The Commonwealth Bank of Australia pleaded guilty in October to 30 criminal charges in relation to mis-selling credit insurance after irregularities were uncovered during a case study as part of the Royal Commission.

This was the first time ASIC had pursued criminal penalty proceedings against a bank. In another case, Allianz Australia, was ordered to pay A$11.5 million for "misleading and deceptive conduct" when selling travel insurance.

Quality of advice

Conflicts of interests left to fester can lead to the demise of an organisation. Boutique wealth management firm Dixon Advisory recently filed for voluntary administration, citing a million-dollar regulatory fine and mounting liabilities brought about by class action suits for alleged failure to act in customers' best interests. Dixon Advisory had been embattled for some years, plagued by bias in selling its own high-risk U.S. fund collateralised products to customers. The firm failed to disclose its interest in significant fees earned, which at one stage accounted for two-thirds of its revenue.

4

Mis-selling products and quality of advice

This case, along with many others, has cast doubt on the vertical integration model still used by many firms in the region . The model allows firms to earn fees from products they market, leading to multiple conflicts of interest, while the high turnover of assets or products makes it difficult for consumers to withdraw from underperforming products.

Many firms still operate a tick-box compliance process which makes it difficult to supervise conflicts of interests or assess a client's best interest. Compliance professionals must consider whether a system based on product renumeration can be self-regulated while at the same time managing the many conflicts that arise.

The case has reinforced the need for regulators to consider advisers' remuneration structures. All-too often, these are driven by sales culture and are not conducive to providing quality advice.

Regulators have long emphasised the need to protect vulnerable customers or those with special needs. Compliance practitioners must ensure the firm designs and distributes its products in a way which caters for the needs of such customers.

Tips for compliance professionals

- Consider the need to assess conflicts of interests in selling products to customers.
- Has there been full disclosure of fees?
- Is the promotional information provided to customers clear and unequivocal?
- Are internal product structures susceptible to conflicts of interest and are there compliance systems in place to review concerns?
- Are customers ineligible from making claims in relation to products they have purchased?
- Are procedures in place to check and review algorithm calculations linked to financial products, to ensure customers are not overpaying?
- Are staff properly trained or upskilled when selling new financial products to customers?
- Are material compliance oversights disclosed with candour to regulators within required timelines?
- Beware tick-box compliance.

5

Climate and environmental, social and governance and diversity, equity and inclusion

In 2022, climate change and environmental, social and governance (ESG) will continue to be priorities for regulators in the region, with climate concerns set to surpass corporate governance as one of the most pressing concerns for investors. COP 26 established several new commitments for Asia-Pacific countries that will change both the way firms look at investments and the basis for lending money to customers.

Various jurisdictions are launching guidelines to help financial institutions manage the risks associated with the transition to a green climate economy. Regulators in Australia, Singapore, Hong Kong and Malaysia are already formulating policies to assist firms with ESG. Some have introduced reporting obligations and guidelines for ESG disclosures.

In 2021, the International Financial Reporting Standards (IFRS) Foundation announced the creation of the International Sustainability Standards Board (ISSB), which aims to address concerns about the quality and consistency of ESG reporting. One such concern is the lack of a consistent taxonomy. The European Union has introduced a classification system that establishes a list of environmentally sustainable activities. Financial institutions in Asia-Pacific need to develop their own framework for making ESG disclosures and must agree on the implementation of environmental taxonomies.

5

Climate and environmental, social and governance and diversity, equity and inclusion

Firms worldwide are working toward diversity, equity and inclusion policies. In 2021, a world business survey found that 79% of major organisations across a variety of industries were planning to devote more budget and resources to DEI. This approach included remote and flexible working conditions, including the need to ensure remote employees are not disadvantaged. It also highlighted the link between DEI strategies and employee retention.

Firms need to take care with their voluntary or mandatory ESG disclosures and develop ESG strategies which guard against accusations of greenwashing from regulators, shareholders and stakeholders.

Tips for compliance professionals

- Boards and senior management need to develop ESG disclosure frameworks.
- ESG strategies need to diffuse potential risks on the horizon.
- Assess and manage emerging ESG issues.
- Ensure appropriate disclosure of the financial alignment between company investments and ESG considerations.
- Assess whether ESG issues will affect supply chain outlets to customers.
- Ensure sufficient staff are trained and/or upskilled in ESG/DEI.
- Is the organisation sufficiently inclusive?
- Devise a DEI strategy.

6

Workplace health and safety

The pandemic has opened a Pandora's box of risk management concerns for employers. Many financial institutions have allowed staff to work remotely during the height of the pandemic, but some are now requiring staff to return to the office. Firms must have procedures to assess and manage the risks to employees of returning to the workplace, including a work health and safety plan which can be updated to reflect new developments.

Firms must also decide how to deal with unvaccinated staff. Some employers have made it mandatory for staff to be vaccinated if they are to work for the organisation, while others remain undecided. Citigroup, for example, is set to begin enforcing its "no jab, no job" policy, making it the first Wall Street bank to dismiss unvaccinated workers despite there being no government imperative to do so. Many firms are struggling with the intersection between making vaccination compulsory and the individual rights of employees.

Of particular concern is that a firm's stance on vaccination may lead it to become embroiled in litigation. The politicisation of differing anti-vaccine views following Australia's deportation of Novak Djokovic - despite the player having been granted an exemption by Tennis Australia Pty Ltd - has brought these concerns into sharp focus.

Tips for compliance professionals

- Is the firm's health and safety policy able to deal with staff returning to work?
- Is there sufficient provision to ensure remote employees are not disadvantaged, and to ensure diversity of employee retention?
- Are employees' rights adequately balanced with vaccination imperatives?
- What litigation might the firm potentially face following its decisions in this area and how will that affect resources?

7

Management accountability

Senior management accountability remains a strong focus for Asia-Pacific regulators. Personal accountability regimes have now been operating for three years in the region, but it is unclear just how effective they have been. Despite some large regulatory fines and high-profile litigation, few senior individuals have been held to account for compliance failures, leading some to question the extent to which such regimes represent a credible deterrence.

Non-financial misconduct

It sometimes used to appear that there was one rule for executives and another for rank-and-file workers. A dichotomy has begun to emerge however, whereby senior executives are increasingly being dismissed or stood down for non-financial misconduct which has taken place outside the workplace.

Behaviour as diverse as breaching COVID-19 protocols, having a friendship with a high-profile convicted paedophile and sexually harassing a colleague at a social function has all led some senior executives to be deemed not "fit and proper" to continue in their management roles. For example, Antonio Horta-Osorio, chairman of Credit Suisse Group, recently resigned when he breached COVID-19-related rules by using a corporate aircraft, and for having attended the Wimbledon tennis finals when he was supposed to be in quarantine.

Firms have become increasingly mindful of the need for a strong culture and have come down hard on those senior executives found to have breached codes of moral and legal conduct, no matter how small. This has also led to questions about whether firms are appointing the right individuals to these positions in the first place.

What is very clear is that firms are taking "social misconduct" more seriously and seeking to protect their reputations. The personal accountability risk landscape for senior managers and executives has evidently expanded into moral and ethical issues outside work.

Tips for compliance professionals

- Is the organisation hiring the right senior executives in terms of integrity and honesty?
- Are the organisation's cultural expectations reflected in senior managers' conduct and employment contracts?
- Does the organisation provide appropriate training or "time out" discussion for senior managers to assess evolving issues of senior management responsibility and organisational culture?
- Does the organisation insist employees participate in a compulsory training course on ethics?
- Does the whistle-blower system work?

8

Digital transformation

Digital transformation is happening at pace. Online banks and fintechs offer a wide range of financial services that leverage technology to develop a competitive edge in products offered to customers in Asia.

Firms involved in, or planning, digital transformation need to be aware of the risk and compliance difficulties that advanced technological platforms can introduce and understand the vulnerabilities they can create for both customers and the organisation. Digital transformation needs to be accompanied by improvements in culture, conduct risk, data protection, privacy, cyber security, staff training , risk management and third-party outsourcing.

Many customers now rely on social media to receive communications, and while this will only expand in the next five years, a significant number - including vulnerable customers - are not IT-savvy and find it hard to use technology that is not user-friendly. Financial institutions must bear this in mind when designing digital platforms and provide support for vulnerable customers.

There is also concern that, in parts of the financial sector, digital transformation is "outpacing" regulation, and this too has helped accelerate governments' plans to introduce new rules for fintech firms.

Tips for compliance professionals

- Are customers' needs being adequately considered?
- Are the risks to customers considered adequately when developing digital products?
- Is the compliance team involved at the design stage, and is it part of strategic decision-making?
- Has the organisation implemented effective user-friendly controls over social media communications?
- How can the organisation use digital transformation to improve customer satisfaction, service and trust?

9

Regulatory over-reach and overload

The number of initiatives, rules, laws and guidelines issued by regulators has accelerated at an unprecedented pace, making it increasingly difficult for compliance professionals to keep abreast of developments. The pandemic has only intensified regulators' determination to focus on organisations' operational resilience.

A particular concern is the growing lack of regulatory coherence across jurisdictions, which makes it harder and more expensive to do business. For example, by complying with U.S and EU sanctions on China, companies face the possibility of tough sanctions in China. As discussed above, crypto trading has no agreed taxonomy; it is banned in China but allowed to a limited extent in other parts of Asia. Data protection laws also differ materially across jurisdictions.

Compliance professionals must focus on whether internal compliance controls are working and are in line with regulatory guidelines. Compliance needs to be fully involved in the organisation's plans to manage risk and to protect the interests of both customers and the organisation as whole.

Tips for compliance professionals

- Ensure that senior management have up to date regulatory intelligence about issues that may impact the firm?
- Ensure there is sufficient training for staff training or discussion on emerging issues.
- Consider what measures can be taken to improve compliance capabilities in areas of risk?
- Provide feedback to regulators about regulatory overreach and overload so guidelines are more streamlined.

10

Skills, talent and knowledge

Organisations and regulators alike are finding it increasingly hard to attract and retain suitably qualified staff. The shortage of skilled, experienced AML staff could become a real threat for organisations, to the extent where it might affect the conditions of their regulatory licence.

Organisations need to identify the skills they need most. One option then would be to hire capable staff who, while they may lack the full range of skills, can be retrained. Another option would be to upskill existing staff. Firms may also need to move skilled staff into different areas to fill gaps and make arrangements to provide employees with continuous training to ensure operational resilience.

Tips for compliance professionals

- Identify the skills that will be most valuable in future for the organisation.
- Employ people who can attain those skills and provide technology-linked learning and on-the-job training.
- Develop a road map for improving compliance capabilities and improving skills.
- Implement upskilling programs where skills gaps are identified.
- Consider that a lack of training can contribute to failures to adhere to applicable regulatory requirements.
- Is your organisation placing enough emphasis on integrity and honesty qualities when hiring staff?

ABOUT THE AUTHOR

Niall Coburn is the regulatory intelligence expert for the Asia Pacific region for Thomson Reuters. He was a Senior Specialist Adviser to the Australian Securities & Investments Commission (ASIC) and Director of Enforcement for the Dubai Financial Services Authority (DFSA). Niall was part of an international team that wrote the regulatory and financial market laws and rules for the Dubai International Financial Centre.

Niall is a Barrister of the High Court of Australia and has over twenty years experience in financial markets and international regulation. In 2002, he was awarded an ASIC Australia Day Honour Medal for his work in corporate investigations.

He has worked in Europe, Middle East and Asia with financial institutions, liaising with international regulatory bodies, government agencies and corporations. Niall has published extensively on compliance and financial regulation internationally and written a book on corporate investigations published by Thomson Reuters and has been a commentator in the Australian Financial Review and television on financial crime, regulation and compliance.