INSIGHT

How to manage compliance risk and stay out of the headlines

Thursday 17 February 2022

Compliance risk has traditionally been the poor cousin of longer-established risks to financial services organisations, such as credit and market risk. But that's no longer true. Recent high-profile compliance risk failures have made headlines, with businesses having to pay record fines, board chairs and CEOs being forced to resign, and reputations being damaged, resulting in reduced trust from customers and the community.

Managing compliance risk can be tricky. When APRA-regulated entities are managing compliance risk well, fewer and less severe regulatory breaches arise, meaning less time is required for remediation, and business runs smoothly. But if organisations don't have systems in place to properly manage compliance risk, the outcomes can be disastrous. Recent high-profile compliance failures show that failing to manage compliance risk can cause severe financial and reputational damage.

Examples of failures that have attracted significant fines, along with reputational damage for businesses include: failure to correctly treat customers (including charging deceased persons, double charging for products, and not applying package discounts), failure to meet anti-money laundering obligations, and privacy breaches. In a number of instances, the organisations in question admitted to shortcomings in their processes, systems, and monitoring to avoid or provide early detection of breaches.

In late 2019, APRA completed reviews of the four major banks, with a focus on compliance risk management. Since then, APRA supervisors have increased attention on how entities across all industries are managing compliance risk, the challenges they face in doing so, and how their practices in this key area can be improved. And there is still room for improvement when it comes to entities' management of compliance risk – across all APRA-regulated industries – with APRA's regular supervisory engagement reinforcing the observations from its 2019 reviews.

What is compliance risk?

Broadly speaking, compliance risk relates to an organisation's ability to comply with the laws, rules, regulations and standards (both external and internal) which govern its operations – including voluntary industry standards and codes of conduct that an organisation elects to comply with – and the consequences that may flow if it fails to do so.

While operational risk looks at understanding and managing the risks associated with the achievement of strategic objectives, the related topic of compliance risk can be considered as managing minimum requirements and the 'ticket to play' of a business.

Each organisation's compliance obligations will be driven by the industry in which it operates, and the products and services it offers. As there isn't a single consolidated set of obligations that a financial services organisation must follow (given the diversity of activities that different financial services organisations are involved in), businesses need robust processes to identify relevant obligations and keep up-to-date with regulatory change.

While there are typical obligations that financial services organisations must comply with (such as APRA's prudential standards), overall compliance management will often be aligned to the organisation's industry, the products and services it offers, and its approach to risk management.

APRA's approach to compliance risk

To maintain trust in Australia's financial services industry, it's essential that compliance risk management remains a priority for senior management and boards. A well-documented approach to compliance risk management supports an APRA-regulated entity's operations. It allows the entity to spend more time creating value for, and having meaningful interactions with, customers, instead of dealing with the consequences that can arise due to non-compliance with laws and other obligations, including reputational damage. An entity's management of compliance risk can also provide a barometer of its approach to risk management generally.

While a number of regulators – both in Australia and overseas – supervise and enforce different elements of an entity's compliance management practice, APRA's interest is particularly on an entity's ability to demonstrate and monitor compliance with prudential standards, and to consider APRA's guidance. When there's a breach of a prudential standard, APRA focuses on the people, systems and processes that have contributed to the incident to ensure the underlying cause has been identified and addressed.

APRA also looks at an entity's ability to meet non-prudential obligations and laws as a way of gauging the adequacy of entities' risk frameworks, and risk management processes and practices. APRA considers an entity's compliance risk management processes to understand how the entity captures and maintains its obligations, and ensures adherence to those obligations. This helps inform APRA of the suitability of the entity's risk management framework to manage risk.

Prudential Standard CPS 220 Risk Management sets out APRA's requirements in relation to the risk management framework of an APRA-regulated institution. CPS 220 specifically requires that entities have an adequately staffed, appropriately trained compliance function, with a reporting line independent from business lines.

APRA's recent supervision has examined larger and more complex entities and their attention to, and progress on, addressing issues in managing non-financial risk, specifically:

- their compliance management strategy,
- their implementation of frameworks and systems, and
- their accountability and oversight mechanisms to support their strategy.

The key observations from this work have highlighted the need for entities to:

1. Have a clearly **defined approach** to managing compliance risk,
2. Have **established processes** to support compliance risk management practices, and
3. Specify **clear accountability** for managing compliance risk.

Defined approach

APRA has observed that entities face challenges in developing and maintaining a complete view of obligations that apply to their business operations. Even when entities use regulatory compliance subscription services, complexities arise – such as identifying all relevant obligations, and the need to manually supplement the information provided by subscription services. This complexity is

compounded when entities operate across multiple jurisdictions, which creates multiple sets of regulatory and prudential obligations for them to identify, maintain and follow.

Better practice by entities involves a hybrid approach, including a mix of subscription services and input from compliance subject matter experts, to ensure that all obligations are captured and regularly updated. This hybrid approach is enhanced when representatives from different business units and the compliance function work together to maintain a detailed understanding of all end-to-end processes. Better practice also involves the business units and the compliance function coordinating their approach to plan for, and manage, any changes to obligations – including any major regulatory changes – to ensure the entity is compliant in time.

Established processes

APRA has observed that while entities recognise the need to understand the processes associated with their product and service offerings, it can be challenging to implement and maintain an accurate view of these processes. Entities that have moved closer to documenting their end-to-end processes are able to overlay compliance obligations on their processes, allowing them to identify gaps and then fill those gaps in order to show compliance with obligations.

Better practice involves understanding end-to-end processes for products and services, applying an overlaid view of compliance obligations, and implementing ongoing monitoring to identify any gaps between business process and applicable regulations and laws. This allows business units to understand their current level of compliance and to maintain processes so they are compliant by design. This should be supported by the business unit reporting to senior leadership and the board to present a complete view of obligations compared to the end-to-end process so that gaps can be identified and addressed.

Clear accountability

APRA has observed that there are operating model and resource considerations when managing compliance, and entities that are closer to the adoption of the "Three Lines of Accountability" model are more proactive in monitoring issues as they arise and in actively managing compliance risk. The Three Lines of Accountability is one model that is widely used and provides an effective framework for risk management including:

- the business (Line 1), which is accountable for managing compliance risk,
- risk management (Line 2), which provides oversight and challenge, and
- internal audit (Line 3), which performs independent assurance activity.

In many entities, however, accountability for the management of obligations and corresponding controls remains more with Line 2 risk teams than with Line 1 business functions. While instances of better practice are present in more mature entities which continue to invest in people, process and

systems to support compliance risk management across their entity, these are yet to become the norm.

APRA has observed more progress in clarifying accountabilities in the banking industry, no doubt incentivised by the requirements of the Banking Executive Accountability Regime (BEAR). Clear accountability remains a key focus for APRA's supervision teams, since failure of Line 1 to take accountability for compliance management limits the ability of the Line 2 risk team to provide meaningful oversight and challenge, as they instead need to step in to the day-to-day management of obligations and controls.

Better practice involves entities creating clear accountability for compliance risk management across the Three Lines of Accountability model, as part of their compliance risk management framework. This will ensure that established processes are implemented. Accountability is further improved when senior leadership and the board foster a culture of treating compliance risk with the utmost importance to set the tone for all staff.

The appointment of a Chief Compliance Officer (CCO) emphasises and gives a voice to compliance management, supporting CPS 220's requirement for an independent compliance function. In the absence of a CCO role at senior leadership levels, it is essential that mechanisms are in place for the voice of compliance to be heard in executive and board discussions, and that compliance is championed by senior leaders of the organisation.

Where to from here?

Better practice for compliance risk management will continue to be a focus area for APRA, and is a key consideration across the Australian financial services sector for both industry participants and regulators. APRA wants to see regulated entities giving the same attention and prioritisation to compliance risk management that they give to cyber risk, operational risk management and other risk classes. Evidence has shown that compliance breaches can be extremely costly.

While APRA has observed entities' investment in people, systems and processes to support the management of compliance risk, high profile events and the subsequent failures of compliance monitoring practices highlight the continued importance of strong attention from senior leadership and boards.

Entities across all industries should ensure they have a defined approach, established processes and clear accountability to manage compliance risk. APRA will continue to closely monitor entities' management of compliance risk through its supervisory activities.

The Australian Prudential Regulation Authority (APRA) is the prudential regulator of the financial services industry. It oversees banks, credit unions, building societies, general insurance and reinsurance companies, life insurance, private health insurers, friendly societies, and most members of the superannuation industry. APRA currently supervises institutions holding $6 trillion in assets for Australian depositors, policyholders and superannuation fund members.