Living the Code

Embedding Code obligations in compliance frameworks

June 2020

GENERAL INSURANCE
Code Governance Committee

Contents

Chair’s message

In the wake of the Financial Services Royal Commission, the General Insurance Code Governance Committee was left with serious concerns that underreporting of Code breaches reflected deficiencies in Code subscribers’ compliance monitoring frameworks and a failure to take the Code’s obligations as seriously as they should. This has also been an ongoing theme of our compliance data reporting for a number of years, in particular in our recently released *Annual Report: General Insurance in Australia 2018-19 and current insights*. Following the Financial Services Royal Commission, we launched an own motion inquiry into the adequacy of subscribers’ compliance frameworks, which confirmed our concerns and led to the preparation of this report: *Living the Code: Embedding Code obligations in compliance frameworks.*

The purpose of this report is to remind insurers that, by subscribing to the Code of Practice, they must implement and maintain a culture of fairness and honesty that prioritises the needs of consumers and small businesses. As Commissioner Hayne remarked in his Final Royal Commission Report, industry codes are expressed as promises by industry participants – promises that must be made seriously if the codes are to be anything more than “public relations puffs”.

Complying with the Code is not about ticking boxes and meeting minimum standards. It requires subscribers to make an active commitment to:

- a culture that enables honesty and fairness at all levels of the organisation
- strong leadership on matters of honesty and fairness; and
- robust governance and business practices, systems and processes.

Each of these interrelated areas forms a chapter of *Living the Code*. We look first at the importance of developing a strong organisational culture that places the Code, and the Code’s purpose of doing the right thing by consumers, at the heart of all strategy and decision-making. We then focus on the need for those at the top of insurance organisations to ‘set the tone’, by role-modelling the desired behaviour and advocating a Code-first approach throughout the business. Finally, we examine the governance processes that are required to encourage and enable people to meet their compliance obligations and ‘live the Code’.

This report, like all of our publications, is an important resource for everyone who works in the general insurance industry. It makes particularly compelling reading for those who sit on Code subscribers’ Boards, as it provides valuable insight into industry trends and issues, as well as recommendations for achieving best-practice Code compliance.

The need for Boards to improve their oversight of non-financial risks was called out in both the Royal Commission’s Final Report and APRA’s Information Paper on Self-Assessments of Governance, Accountability and Culture. Without access to the kind of information contained in this report, Boards may remain in the dark and may not lead effectively on non-financial risk and compliance matters.

The Committee was therefore disappointed to learn as a result of the own motion inquiry that breach reporting is not reaching the Boards of some subscriber organisations, and that only a handful of Boards are being provided with the Committee’s reports and recommendations for improving Code compliance.

Demonstrated compliance with the Code is more critical than ever in light of the Government's post-Royal Commission proposal to make some Code provisions enforceable. As Commissioner Hayne warned financial services entities in his Final Report, if they don't start taking their Code obligations more seriously, they will lose the right to self-regulate.

The fundamental purpose of insurance is to protect people against adverse and unexpected events. This has never been more evident than the current worldwide experience of the effects of the Coronavirus pandemic. The Committee's advice to insurers is this: do the right thing, put your customers first, and embrace the opportunity to embed a strong culture of fairness, honesty and transparency by implementing the recommendations in this report. That commitment has never been more important.

The commencement of the new 2020 General Insurance Code of Practice is an ideal opportunity for subscribers to assess their culture and align the values of their organisation with the values in the new Code, which has been updated to enhance consumers' understanding of their rights, while clarifying insurers' obligations to consumers. It also gives subscribers a chance to assess the robustness of their compliance frameworks to ensure they can meet their obligations under the new Code.

The Committee thanks all the Code subscribers who took part in the own motion inquiry and shared their APRA self-assessments with us. It has been pleasing to note that monitoring and reporting of breaches by subscribers has improved since we commenced the inquiry, and we expect to see further improvements as subscribers implement the recommendations in this report and transition to the new 2020 Code.

Lynelle Briggs

Lynelle Briggs AO
Independent Chair
General Insurance Code Governance Committee
June 2020

The own motion inquiry

The breach and significant breach data collated as part of the own motion inquiry suggest weaknesses in many subscribers' compliance frameworks. Unusual volatility in some subscribers' breach numbers over the five-year reporting period highlights the impact of changes to monitoring and reporting approaches. At the same time, low numbers of self-reported breaches and significant breaches suggest that many subscribers' compliance frameworks are failing to capture breaches of the Code.

Scope and methodology

In 2017-18, the Financial Services Royal Commission asked the Committee to provide information about trends in subscribers' breaches from 2014 to 2018. Compiling and analysing this data gave the Committee an opportunity to reflect on subscribers' Code compliance and reporting over the four-year period. The Committee concluded that subscribers overall were underreporting instances of Code breaches and that breach numbers across the four years were inconsistent, fragmented and questionable – potentially indicating weaknesses in subscribers' compliance monitoring and governance frameworks.

The Committee's overarching concern was that these weaknesses were an indication that some subscribers had an insufficient grasp of the scope and understanding of the Code's true purpose, or that they were not taking their Code obligations seriously. In light of this, the Committee launched an own motion inquiry in September 2018 to investigate the adequacy of subscribers' compliance frameworks.

The inquiry began when a group of 45 subscribers that had reported breach data in the last four financial years was asked to respond to questionnaires. These subscribers were required to provide the Committee with a report that:

- analysed their breach data
- explained how they test the effectiveness of their compliance monitoring and reporting frameworks, and
- explained how Code-related issues are addressed at executive management and Board level.

SHARING APRA SELF-ASSESSMENTS

All 45 subscribers were asked to consider sharing the outcomes and findings of their APRA self-assessment[1] review with the Committee, if they completed one. In response, **nine** subscribers provided documents to the Committee,

  - including **three** of the general insurers that APRA had specifically requested to complete a self-assessment.
  - The other **six** subscribers who provided a response to the Committee were among those who voluntarily elected to conduct a self-assessment.

- **One** subscriber provided insights from its group's self-assessment that applied to it specifically.
- A further **six** subscribers did not provide documentation but agreed to meet with the Committee to discuss their self-assessment.
- Another **nine** subscribers had not been asked by APRA to complete a self-assessment but had nevertheless carried out their own internal or external reviews and all agreed either to provide documentation or meet with the Committee to discuss it in further detail.
- A further **four** were undertaking a review (either in their own right or as part of their group) but it was not yet complete.
- The remaining **16** did not undertake a review/self-assessment.

[1] Following the release of its Prudential Inquiry into the Commonwealth Bank of Australia, APRA called on all APRA-regulated institutions to reflect on the findings and consider whether similar issues might exist in their own organisations. APRA also wrote to the Boards of 36 financial institutions, including nine general insurers, asking them to conduct a self-assessment against the findings and provide that assessment to APRA.

RESPONDING TO THE ROYAL COMMISSION

In August 2019, a follow-up questionnaire was sent to and completed by 10 of the 45 subscribers that were of varying sizes in order to:

- gain further insight into, and assess the robustness of, their incident and breach reporting frameworks, including how significant breaches of the Code are identified and ultimately prevented
- gain insight into the extent to which the outcomes of the Financial Services Royal Commission have stimulated cultural change within subscribers' organisations.

The findings of our own motion inquiry validated the Committee's concerns about weaknesses in subscribers' compliance frameworks and highlighted issues or potential issues from a cultural, leadership and governance perspective in many subscribers' organisations that indicate subscribers are not "living the Code".

Accordingly, the scope of the report widened to incorporate commentary on the Committee's expectations around culture, leadership and governance, as well as recommendations on how subscribers can improve in these areas.

The questionnaires sent to subscribers can be found at Appendix 1.

The Code as a blueprint

The General Insurance Code of Practice (the Code) requires insurers to provide high standards of service in an honest, fair and transparent way. However, the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (the Royal Commission), APRA's Prudential Inquiry into the Commonwealth Bank of Australia, and the Committee's own motion inquiry have shown that not all insurers are doing so. Many are breaching the Code.

This *Living the Code* report has been produced to help insurers adhere to the Code. Adhering to the Code is not just a matter of ticking boxes and meeting minimum standards. As the Committee has consistently stated, one of the most important messages to come out of the Royal Commission was that to be fair, honest and transparent in dealings with customers, the financial services industry needs to go beyond bare minimum requirements to act in the spirit of the law. The rules are a baseline, but industry needs to go much further.[2]

We want insurers to act in the spirit of the law and the Code so that the insurance industry achieves real reform[3]. Such reform will mean the financial services sector regains the trust and confidence of consumers.

Key findings

This section of the report summarises the key findings of the own motion inquiry, which the Committee has discussed throughout this report.

The Committee's findings from the own motion inquiry varied. There was evidence of good practices but also of inadequate practices even among the larger, more sophisticated insurers.

ABSENCE OF BOARD AWARENESS OF COMMITTEE GUIDANCE ON CODE COMPLIANCE

The Committee expects its reports and recommendations to be distributed to all levels within subscribers' organisations, including their Boards – yet it is clear from subscribers' responses to this own motion inquiry that this is not happening. Just six of the 45 subscribers who took part in this inquiry said they provided some of the Committee's publications directly to their Boards and even then, most could not specify which publications their Boards had seen.

[2] General Insurance in Australia 2017–18 and current insights, General Insurance Code Governance Committee, p. 3.

[3] Annual Report: General Insurance in Australia 2018-19 and current insights General Insurance Code Governance Committee, p.7

SPIRIT OF THE CODE, HONESTY, FAIRNESS AND TRANSPARENCY

In some instances, subscribers are reverting to black letter law in response to the Financial Services Royal Commission, an approach that is clearly not within the spirt of the Code or the law.

Some subscribers' responses point to weaknesses in compliance and reporting frameworks that represent an insufficient grasp of the scope and understanding of the meaning of the Code. Some of these weaknesses include a poor understanding of standards:

- that contain elements of honesty, fairness and transparency,
- the meaning of "significant breach" and
- the related obligation to report significant breaches to the Committee within 10 business days of identification.

BOARD AWARENESS OF BREACHES

Some subscribers, including large subscribers with apparently comprehensive compliance frameworks, are reporting surprisingly low numbers of breaches. Yet these larger subscribers reported that their Boards have Board Risk Committees or forums to which significant breaches (and in some cases, all breaches) are reported.

There was considerable variability in the nature and comprehensiveness of breach reporting to Board Risk Committees. Some subscribers described processes by which the Board actively reviews and challenges breach data. However, some smaller subscribers reported that their Boards do not examine breach data.

COMPLIANCE FRAMEWORKS

Around one-third[4] (33%) of subscribers described a robust compliance framework that meets Committee expectations. These subscribers described comprehensive frameworks adhering closely to the three lines of defence model and were seen as examples of best practice. Another third (33%) described compliance frameworks with some of the elements of a best practice framework, but room to improve. Of the remainder, around 11% described a framework that needs considerable improvement, while around 23% did not describe their compliance framework in enough detail.

Deficiencies in the three lines of defence model included: a lack of clarity between roles and responsibilities; inadequate resourcing of Line 2 functions; too few compliance staff; weaknesses in risk-management systems and processes; and an absence of the Line 3 audit function.

IDENTIFICATION OF BREACHES AND SIGNIFICANT BREACHES

Some subscribers are adopting a lax attitude to breach and significant breach identification, and to investigating the root cause of breaches.

In some cases, subscribers are reporting incidents as Code breaches, only for the Committee to determine after further investigation that they are not, in fact, Code breaches. This is evidence of a lack of rigour in subscribers' processes for identifying and reviewing breaches. Subscribers routinely attribute non-compliance with the Code to human error or the result of an individual's actions without demonstrating that they carried out a deeper examination of root causes and of the problems that led to the breaches.

In other cases, subscribers are failing to correctly identify multiple breaches connected to the same underlying cause as a reportable significant breach, instead including them as standard breaches in their annual report of breach data to the Committee. This points to a failure by subscribers to understand and interpret the definition of a "significant breach" as set out in section 15 of the Code and to an unwillingness or unpreparedness to review breaches for evidence of systemic failings and major problems.

[4] Figures have been rounded up to nearest whole percentage number.

CONTROLS

While some subscribers described processes for reviewing or testing the controls that are in place to ensure that breaches are prevented or detected, recorded, reported and addressed appropriately, there was marked variation in the comprehensiveness of subscribers' descriptions of their controls. In many cases, these descriptions were not detailed enough for the Committee to be confident that controls were sufficient.

Smaller organisations and teams tended to have less formal control arrangements. These organisations and teams must implement appropriate control arrangements to minimise the risk of breaches.

CODE AWARENESS

Given the low levels of breaches identified by subscribers, all subscribers need to do more to improve Code awareness amongst their staff and third-party distributors. But improving Code awareness does not come simply from training. Rather, it comes from embedding a culture where Code compliance is demonstrably "lived" through the decisions and actions of all staff and distributors, and not just treated as a box-ticking exercise at reporting time.

Subscribers must engage their staff and distributors to understand that the Code should be at the heart of everything they do on the subscriber's behalf.

Recommendations

To address the deficiencies identified in the own motion inquiry and help subscribers embed the Code obligations into their compliance frameworks, the Code Governance Committee has made the following recommendations.

BREACH AND SIGNIFICANT BREACH REPORTING

1. Take breach identification and reporting seriously. Ensure you have in place rigorous processes for identifying and reviewing breaches. Confirm Code breaches before reporting them to the Committee.
2. Review incidents and breaches to see if they are significant breaches. Assess them against the significant breach criteria in section 15 of the Code. Consider each factor identified in the definition and take a broad view. If in doubt, err on the side of caution and report a 'possible significant breach' to the Committee.
3. Use a systemic issue identified by AFCA in a complaint, or a significant legal breach identified by ASIC, as a trigger to examine whether the matter is also a significant breach of the Code.
4. Review and analyse your internal complaints and disputes register and complaints that AFCA or regulators receive about you to identify trends and emerging issues and report significant breaches.
5. Examine and record the root cause of all incidents and breaches to determine any trends or patterns. If multiple breaches share the same root cause, they are likely to be a significant breach and must be reported to the Committee.

CULTURE

6. Assess your culture, make the necessary changes, and assess again. Keep doing this.
7. In your values and practices, be clear about what is acceptable behaviour for your directors, senior executives and employees. Then enact and enforce those values and practices. Ensure meaningful consequences for unethical behaviour and misconduct.
8. Focus on developing trust and psychological safety across your organisation. Create a culture where breach reporting is seen as a positive thing and support people who alert you to Code breaches and potential compliance issues.
9. Put the consumer at the centre of your thinking. Hear the consumer voice within your organisation. Ask what you can do to help your customers and create the best possible outcomes for them.
10. Make sure your measurement and reward systems do not focus solely on short-term profit. Do not reward behaviours that may be associated with unethical behaviour.
11. Align your remuneration with consumer-centric cultural values. Reward desired behaviours and good outcomes for customers, not just profit. Include non-financial performance metrics and apply this at all levels of the organisation.

12. Prepare now for APRA's proposed changes to CPS 511. Review how staff are incentivised and ensure non-financial performance measures are given equal weight to financial performance measures.
13. Align the values of your organisation with the values in the Code. Then make sure norms and behaviours in your organisation align with those values.

LEADERSHIP

14. Invoke a culture of collaboration and unity by enabling Board members and executive management to regularly spend time with staff across the business. Let them watch how staff function on a day-to-day basis. Make it possible for them to listen in on customer calls across the entire value chain, including complaints. Encourage both parties to raise any issues or concerns about Code compliance.
15. Report all breaches to the Board, not just significant breaches. Report at least monthly and allow for significant breaches to be reported as they happen. Give Boards access to online breach registers so they can extract reports in real time.
16. Alert your Board or delegated sub-committee to the Code Governance Committee's publications. Highlight key findings, observations and recommendations and explain how these are relevant to your business and its Code compliance obligations.

GOVERNANCE AND PROCESS

17. Include a robust three lines of defence model in your risk management framework that is actively championed by the Board. Always include the third line function, no matter how small your organisation. Clearly define each line function's roles and accountabilities so that individuals understand their responsibilities and facilitate regular meetings between lines to reinforce this.
18. Automate controls so that breach alerts and reporting do not rely on manual intervention. Have systems with built-in triggers for Code requirements relating to timeframes.
19. Embed a consumer-centric culture where staff understand the values of the Code and their obligations to consumers. Explain why and how staff must report Code breaches. Do this when onboarding new staff and follow it up with regular 'refresher' training. Assess the effectiveness of your staff training and monitor the outcomes for any gaps or deficiencies.
20. Make it easy and blameless for staff to report incidents and Code breaches. Encourage them to see breach reporting as a good thing – a chance to 'right a wrong' and prevent it from happening again.
21. Ensure your distributors and service suppliers are fully aware of the Code and their compliance obligations. Check that they know how to identify and report breaches and potential breaches of the Code. Include clauses in their contracts/service level agreements that require this and stipulate the consequences for non-compliance.
22. Invest in compliance-specific staff. Make it their job to conduct comprehensive compliance assurance reviews to identify legislative, regulatory and Code non-compliance.

Breaches

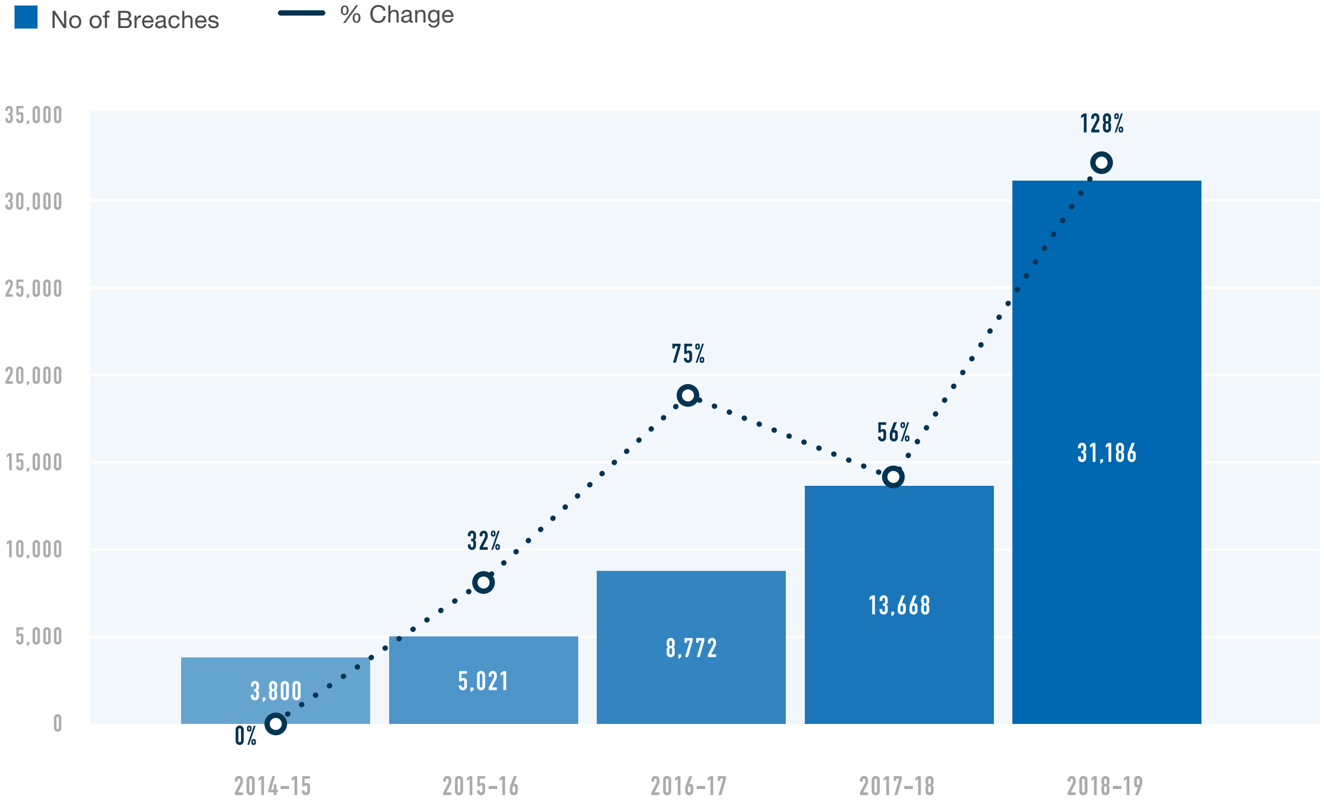
Subscribers self-report breaches to the Committee. Unusual spikes and decreases from year to year, as well as the low numbers of breaches reported by many subscribers, point to past – and in many cases, ongoing – underreporting.

YEAR TO YEAR VARIATION

Over the five years to 2018–19, the numbers of breaches reported by some subscribers have often shifted dramatically from year to year. Two subscribers reported large year-to-year decreases in breaches. Between 2015–16 and 2016–17, one subscriber's self-reported breaches decreased by 90%. Between 2016–17 and 2017–18, another subscriber reported that breaches more than halved. The subscribers reported that these changes reflected a real reduction in breaches as a result of portfolio divestments or deliberate efforts to improve compliance, for example, by improving business processes or hiring more claims staff.

More common than large decreases, however, were dramatic spikes in self-reported breach numbers. This has resulted in overall increases in breaches from year to year **(Figure 1)**.

FIGURE 1: BREACHES REPORTED BY SUBSCRIBERS FOR THE LAST FIVE YEARS[5]



Five subscribers reported that their breaches more than doubled at least once over the five-year period. One subscriber, for example, saw self-reported breaches increase substantially between 2014–15 and 2015–16, followed by further large increases in 2017–18 and 2018–19, when its breaches more than tripled in both of those years.

Explaining the changes, subscribers reported that increases sometimes reflected, at least in part, the impact of natural disasters, increased claim volumes and/or changes to claims systems and processes. Such changes can lead to a higher number of claims-related breaches. For example, where high claim volumes put strain on a subscriber's resourcing, subscribers can fail to meet claims-related timeframes.

However, subscribers tended to attribute spikes in self-reported breaches largely to monitoring and reporting improvements. For example, subscribers explained how planned improvements to business processes and controls, Code awareness, monitoring, quality assurance and data and reporting systems led to better identification of breaches in particular years. While such improvements are positive, they also illustrate the deficiencies of previous monitoring and reporting approaches, which were presumably failing to identify or record many of the breaches that occurred.

LOW BREACH NUMBERS

Many larger subscribers' self-reported breach numbers are substantially lower than the Committee would expect for organisations of their size.

Similarly, many smaller subscribers self-reported very low numbers of breaches over the four years to 2018–19. In a number of cases, low self-reported breaches reflect factors such as small numbers of policies in force, a business focus on wholesale rather than retail insurance, or the Code's limited applicability to the subscriber's particular business. However, the Committee identified around 10 smaller subscribers whose low breach numbers suggest systematic underreporting.

[5] Where figures differ from those published in previous Committee reports, this is due to improvements in the extraction and reporting of data.

One subscriber has reversed its trend of low breach numbers. In 2018–19, this subscriber reported 15,961 breaches, substantially more than it had the previous year, and on its own was responsible for 51% of the 31,186 breaches reported to the Committee in 2018–19.[6]

This subscriber informed the Committee during the year that it had:

- made significant enhancements to its incident reporting management system which simplified its incident reporting process, and improved accessibility so that its employees could raise incidents in a timely manner
- enhanced its governance framework by incorporating a governance stream within its first line risk function, and focused on building the competency of employees so that they could identify and report compliance incidents.

These changes led to an improved and consistent approach to incident reporting across the organisation. The Committee acknowledges that these improvements to incident reporting and increased focus on Code requirements and compliance have contributed to the identification of a substantially greater number of breaches.

CASE STUDY

COMPLIANCE MONITORING AND QUALITY ASSURANCE IMPROVEMENTS SEE SELF-REPORTED BREACHES TRIPLE

Between the 2016 and 2019 reporting periods the subscriber made a range of improvements to its compliance monitoring and quality assurance processes. Its First Line Risk and Compliance Teams developed new ways of working and engaging with stakeholders, while existing employee monitoring and supervision was enhanced, including an increase in the number of reviews conducted. Staff were also encouraged to report incidents without fear, were supported and enabled to be part of the solution.

At the same time, changes were made to quality assurance. An organisational restructure combined previously separate quality assurance teams, which allowed for synergies to be found and the focus on Code compliance to be increased. In the motor area, the quality assurance program was revamped to increase both the emphasis on Code compliance and the number of claims reviewed.

Finally, a new process was instituted to review both internal and external dispute resolution complaint files for Code breaches.

Following these changes, the subscriber's identification and reporting of breaches increased threefold year on year in the reporting years 2016 -17 through to 2018–19.

In view of the continuing low levels of breach reporting by other subscribers, this subscriber's approach should encourage discussion around normalising the reporting of breach data and consistency of approach to breach identification and reporting across the industry. At the same time, all subscribers must ensure that they critically review and verify the accuracy of breach data they intend to report to the Committee. In some instances, subscribers have submitted data which, upon examination by the Committee, was found not to indicate a breach. This is concerning, as it points to a lack of rigour in subscribers' processes for identifying and reviewing breaches.

RECOMMENDATION 1

Take breach identification and reporting seriously. Ensure you have in place rigorous processes for identifying and reviewing breaches. Confirm Code breaches before reporting them to the Committee.

[6] Annual Report: General Insurance 2018-19

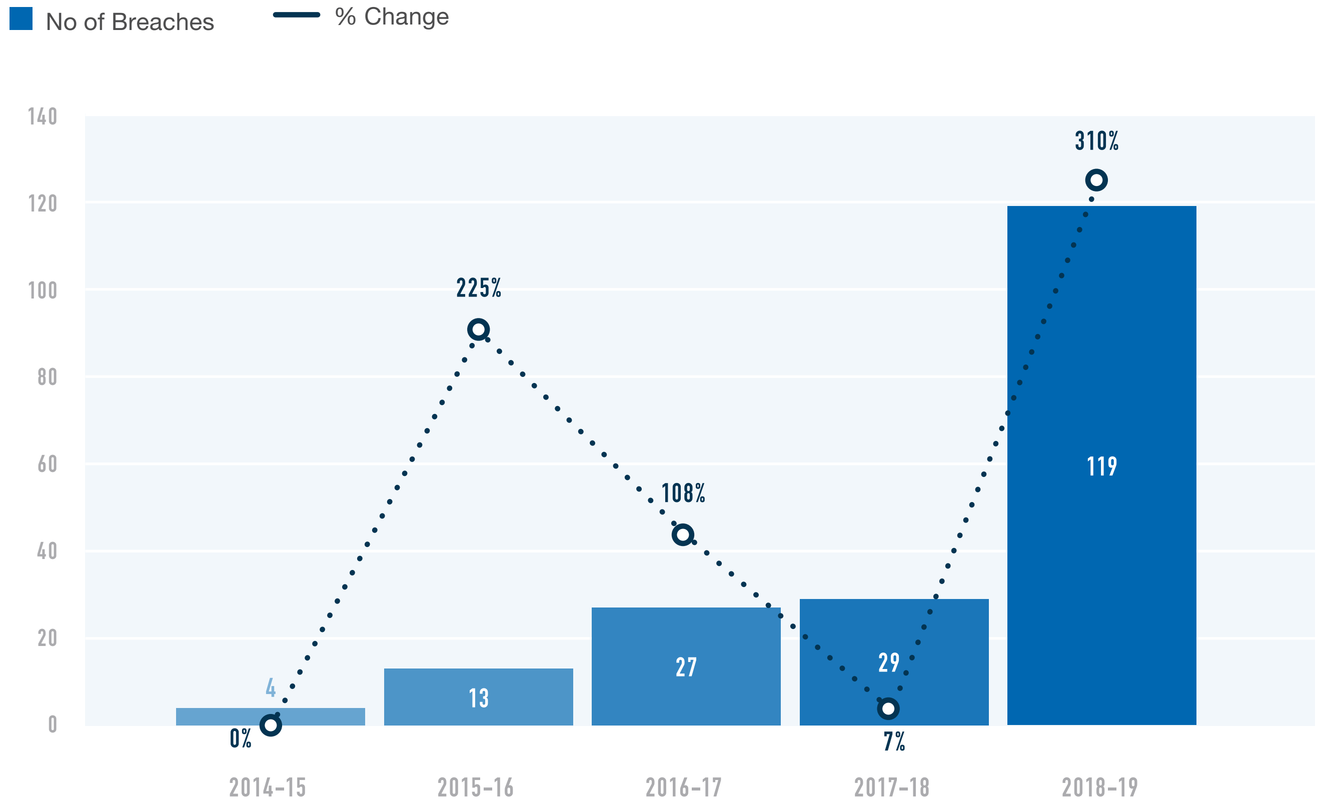
Significant breaches

Under the Code, certain breaches are considered more serious and classified as ‘significant breaches’. A significant breach is one determined to be significant by reference to:

- the number and frequency of previous similar breaches
- the impact of the breach or likely breach on the subscriber’s ability to provide its services
- the extent to which the breach or likely breach indicates that the subscriber’s arrangements to ensure compliance with Code obligations are inadequate
- the actual or potential financial loss caused by the breach
- the duration of the breach.

Subscribers that identify a significant breach must report it to the Committee within 10 business days. However, low numbers of self-reported significant breaches, as well as a recent spike in significant breach reports suggest underreporting of significant breaches. The table below shows that in 2018–19 subscribers reported 119 individual significant breaches, far higher than in any of the previous four years.

FIGURE 2: INDIVIDUAL SIGNIFICANT BREACHES REPORTED BY SUBSCRIBERS FOR THE LAST 5 YEARS[7]



LOW SIGNIFICANT BREACH NUMBERS

Over the four years to 2017–18, many subscribers self-reported very low numbers of significant breaches. While one subscriber has consistently self-reported significant breaches, some larger subscribers reported no significant breaches in most or all of the four years. Similarly, significant breach numbers for smaller subscribers have typically been very low.

Some subscribers have acknowledged that their past significant breach reporting may not have been accurate. One subscriber, although it has consistently reported relatively higher numbers of significant breaches, acknowledged that its framework has been the subject of continuous improvement, and that earlier significant breach reporting may have been incomplete. Reviewing its breach reporting framework, breach data and breach reports to ASIC, one subscriber identified two significant breaches that were not reported to the Committee, and said that it took steps to improve its

[7] Where figures differ from those published in previous years’ reports, this is due to improvements in the extraction and reporting of data.

significant breach reporting framework after identifying deficiencies in late 2017. Similarly, having now reviewed its interpretation of its obligations, its previous breach reports to ASIC and the misconduct identified in its submission to the Royal Commission, another subscriber identified a further 20 significant breaches that were not previously reported to the Committee.

With these few exceptions, most subscribers maintained that they are confident in the accuracy of their reported significant breach numbers and the sufficiency of the frameworks they use to identify and report significant breaches. Subscribers who have not reported any significant breaches to the Committee generally stated that they had reviewed all identified breaches when they were identified and determined them not to be significant.

For a segment of subscribers – namely smaller underwriting agencies and claims administrators that tend to specialise in wholesale insurance – low significant breach numbers are to be expected. However, for many other subscribers, their low levels of significant breach numbers do not align with what would be expected given each organisation's size and consumer exposure. The Committee considers that in many cases, subscribers have been under-reporting significant breaches.

RECOMMENDATION 2

Review incidents and breaches to see if they are significant breaches. Assess them against the significant breach criteria in section 15 of the Code. Consider each factor identified in the definition and take a broad view. If in doubt, err on the side of caution and report a 'possible significant breach' to the Committee.

Over the five-year period to 2018–19, the Committee recorded a number of significant breaches that were not previously identified or reported by subscribers. These significant breaches have been identified by the Committee in its review of internal referrals from AFCA, ASIC media releases and reports from consumer representatives. This indicates gaps in subscribers' own identification of significant breaches of the Code, even in circumstances where the subscriber clearly has knowledge of the matter as it has been the subject of a consumer complaint and/or ASIC report.

RECOMMENDATION 3

Use a systemic issue identified by AFCA in a complaint, or a significant legal breach identified by ASIC, as a trigger to examine whether the matter is also a significant breach of the Code.

From the data available, it is not possible to draw definitive conclusions about the causes of under-reporting. However, it likely reflects a:

- narrow interpretation of the definition of a 'significant breach'
- narrow interpretation of particular Code standards
- lack of a positive reporting culture
- a failure to monitor or examine significant breach activity
- other weaknesses in a subscriber's compliance framework.

RECOMMENDATION 4

Review and analyse your internal complaints and disputes register and complaints that AFCA or regulators receive about you to identify trends and emerging issues and report significant breaches.

RECENT INCREASE IN SIGNIFICANT BREACHES

After reporting few or no significant breaches for a number of years, some subscribers have begun reporting more significant breaches. Having self-reported just three significant breaches between 2014–15 and 2017–18, in 2018–19 one subscriber self-reported 30 significant breaches to the Committee. Similarly, after reporting no significant breaches in four years, another subscriber reported 25 significant breaches in 2018–19. Overall the Committee received reports of 119 significant breaches in 2018-19, an increase of 310% on 2017-18.

The Committee believes that this recent uptick in significant breach reporting is likely to have been prompted by the Royal Commission and the Committee's own motion inquiry, which have boosted subscribers' attention to compliance. It may be the case that before the Royal Commission, there was insufficient focus on significant breaches in many organisations, with subscribers failing to appropriately review breaches and correctly determine whether they should be classified as significant.

RECOMMENDATION 5

Examine and record the root cause of all incidents and breaches to determine any trends or patterns. If multiple breaches share the same root cause, they are likely to be a significant breach and must be reported to the Committee.

An ethical, consumer-focused culture: why, what and how

The Financial Services Royal Commission described culture as ‘the shared values and norms that shape behaviours and mindsets’ within an entity. It is ‘what people do when no one is watching’, and it can either drive or discourage misconduct. There is no single best practice for creating and maintaining a desirable culture; nor can culture be prescribed or legislated. But a good organisational culture is one that values fairness, honesty and transparency, and rewards good consumer outcomes.

Culture and why it matters

A strong culture within a general insurance organisation can prevent misconduct and unethical behaviour.

In his Final Report on the Royal Commission, Commissioner Hayne identified ‘appropriate culture’ as ‘fundamentally important’. Now more than ever, it is also key to the sustainability of an organisation. In the report *General Insurance in Australia 2017–18 and current insights*, the Committee reminded insurers that ‘businesses can accept the challenge of embedding a strong culture of fairness, honesty and transparency, or risk being forced out of business’.[8]

Commissioner Hayne described the ‘culture of an entity’ as ‘the shared values and norms that shape behaviours and mindsets’ within the entity. Culture can drive, or alternatively discourage, misconduct.

The culture of an organisation includes:

- how individuals act and the way they behave
- how individuals relate to each other
- the norms of behaviour within the organisation, and
- the values of the organisation (often unstated as well as explicit).

An organisation’s culture includes both ‘visible’ and ‘invisible’ elements. The visible culture of an organisation is what it commits to doing through policies and strategies, and describes how things are meant to be done. The invisible culture is how people within the organisation actually behave and what they believe about what defines acceptable behaviour. Commissioner Hayne referred to this as ‘what people do when no-one is watching’. The invisible culture of an organisation is just as important as its visible culture – perhaps more so – and is harder to assess and ensure it is positive.

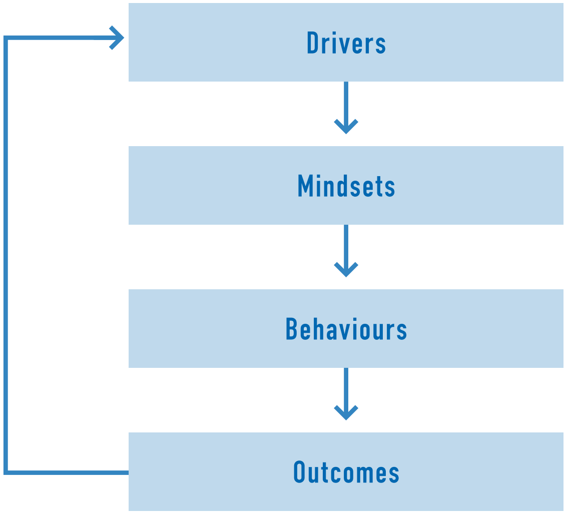
The invisible and visible cultures of your organisation should be aligned and reinforce each other in a positive way. Your organisation’s core values are part of your visible culture and should be reflected in your processes, strategies and decisions. This will help ensure they are in turn reflected in your invisible culture. To ensure a positive invisible culture, it is also important that management, at all levels, models appropriate, ethical behaviour and attitudes.

It is also important to note that culture is not necessarily the same across all areas and people within an organisation – it can and often does change between different work areas and functions. Your aim should be to create a positive culture throughout your organisation, but you may need to approach this differently according to the strengths and weaknesses of different areas and people within your organisation.

[8] General Insurance in Australia 2017–18 and current insights, General Insurance Code Governance Committee, p. 4.

The APRA Prudential Inquiry into the Commonwealth Bank of Australia[9] gave a simple diagram of the key elements of organisational culture:

FIGURE 3: A SIMPLE SCHEMATIC OF HOW CULTURE WORKS



Source: APRA Prudential Inquiry into the Commonwealth Bank of Australia

The Prudential Inquiry report explained the different elements:

> '**Drivers** refer to the context, structures and mechanisms that influence mindsets and behaviours. Drivers take many forms, and can include leadership, policies and procedures, organisational structure, communication, remuneration and group dynamics, as well as the social, economic and regulatory environments. Some drivers, in turn, can be influenced by behaviours or outcomes. This can present itself as a reinforcing loop, demonstrating the interwoven nature of culture.
>
> '**Mindset**s refer to the accumulation of deeply held beliefs, values and attitudes within an organisation. Shared mindsets impact on behaviours, because what people do is influenced by who they are and what they believe and value, whether they are aware of this or not. An example of a shared mindset that often has a negative impact on sound risk management is a view within business units that control functions are an obstacle to be negotiated rather than an important contributor to long-term profitability.
>
> '**Behaviours** are actions visible to others. They encompass how people use their time, communicate and interact with others, and make decisions and trade-offs, amongst others. Behavioural norms emerge when actions become commonplace. It is the grouping of behaviours that impacts on performance or outcomes. An example of a behavioural norm often observed in large institutions that can have a negative impact on sound risk management is a tendency to only escalate "good news"'.

To change culture, organisations must work to change the drivers, mindsets and behaviours of its people at all levels of the organisation. Ensuring a positive culture cannot be achieved through a single effort but rather must be worked at constantly.

It is important to note that a positive culture is necessary but not sufficient to avoid misconduct. Risk management and compliance monitoring are still required. In turn, however, a poor culture will undermine these. A strong culture is inextricably linked to leadership and governance: the other two main sections of this report.

There is no single way to achieve an appropriate culture. The best way will depend on your organisation, its people, and its current culture. However, all insurers can turn to both Hayne's six principles and the Code of Practice itself.

[9] Prudential Inquiry into the Commonwealth Bank of Australia, APRA, p. 82.

What good culture looks like

In a strong culture, Commissioner Hayne's six principles will be the norm for a general insurance organisation and its people. These principles are:

- obey the law
- do not mislead or deceive
- act fairly
- provide services that are fit for purpose
- deliver services with reasonable care and skill, and
- when acting for another, act in the best interests of the other.

In an article titled 'Board Focus for long-term success'[10], John Colvin, Principal of Australian management consultancy Colvin Consulting Group, identified common qualities in companies that have thrived over the long term and have tended not to experience reputation-damaging events. Many of these relate to culture as well as leadership and governance and can be used as benchmarks to assess your own culture:

- a very strong purpose
- a long-term perspective
- a balanced view of who the key stakeholders are
- leaders at Board and executive levels with the appropriate experience, knowledge, character, values and mindset
- leadership that is obsessed with delivering customer value
- driving a very strong innovation culture which focuses on customer needs and improving internal systems and processes
- leadership that is focused on developing a new generation of leaders
- an 'always on' strategy mindset
- active management of a very strong culture underpinned by aligned remuneration and measurement systems.

Risk culture and its relationship to organisational culture

Risk culture is how an organisation and its people approach, understand and manage risk.

In its 2016 information paper on risk culture, APRA said that 'risk culture can be thought of as the impact of organisational culture on risk management'. PwC, in its 2019 *Insurance Risk and Compliance Benchmarking Survey*[11], said that 'risk culture refers to the norms of behaviour for individuals and groups that shape the ability to identify, understand, assess, escalate and act on the risks the insurer confronts, and the risks it takes'.

According to the report from the APRA Prudential Inquiry into the CBA, 'risk culture is not separate to organisational culture but reflects the influence of organisational culture on how risks are managed.'

Like organisational culture, risk culture is a complex mix of behaviours and attitudes within the organisation. Risk culture shapes how an organisation approaches risk management and the kind of decisions it makes around risk. Business risks include financial risks and non-financial risks, such as operational, legal and reputational. The Royal Commission focused on non-financial risks.

A higher risk culture is not necessarily a bad risk culture. However, the decision to take a higher risk approach must be backed up by appropriate risk management and with enough financial backing to bear the consequences if the risk is realised.

PwC also commented that 'a strong risk culture is a unique asset for insurers. It is an enabler to achieving strategy and competitive advantage. It has the power to restore trust and confidence in the organisation.'

[10] 'Board focus for long-term success', John Colvin, Colvin Consulting Group, August 2017.

[11] 2019 PwC Insurance Risk and Compliance Benchmarking Survey, p. 18.

How to achieve a positive culture

Each subscriber is responsible for developing, embedding and sustaining a healthy organisational culture. And because each organisation is different, the actions required will be different for each organisation. However, this report outlines principles that all insurers should follow.

You will first need to assess your existing culture to see where it needs improving. Once you know the problems you will need to identify the best ways to address them. Once you have implemented the changes required, you will then need to assess your culture again to see if the changes have been successful. Then begin the cycle again. Taking these steps means you will meet Recommendation 5.6 of the Commissioner Hayne's Final Report.

Commissioner Hayne also said that 'every entity must ask the questions provoked by the Prudential Inquiry into the CBA'. Many of these related to governance, especially with regard to financial risk, but some related at least in part to culture.

In assessing your culture, you should pay attention to the following:

- Are issues, incidents and risks identified quickly, referred up the management chain, and then managed and resolved urgently? Or is bureaucracy getting in the way?
- Is enough attention being given to compliance? Is it working in practice? Or is it just 'box-ticking'?
- Do compensation, incentive or remuneration practices recognise and penalise poor conduct? How does the remuneration framework apply when there are poor risk outcomes or there are poor customer outcomes? Do senior managers and above feel the sting?

RECOMMENDATION 6

Assess your culture, make the necessary changes, and assess again. Keep doing this.

SET BEHAVIOURAL EXPECTATIONS

Your values and practices should reflect the importance of open, fair and honest behaviour. These values and practices must be lived. Outline your expectations. Model the right behaviour and attitudes. Provide training. And make sure that there are clear consequences for breaches.

RECOMMENDATION 7

In your values and practices, be clear about what is acceptable behaviour for your directors, senior executives and employees. Then enact and enforce those values and practices. Ensure meaningful consequences for unethical behaviour and misconduct.

CREATE A PSYCHOLOGICALLY SAFE WORKPLACE

It is important that people at all levels of general insurance organisations feel safe and empowered to speak out about misconduct or processes, strategies and behaviours that may lead to misconduct and/or breaches of the Code of Practice. This is known as 'psychological safety' and is recognised as being an integral part of a positive organisational culture.

Consider how your organisation will improve psychological safety for your employees. This will include ensuring clear processes for employees to express concerns and report breaches and potential breaches of the Code – and making sure they are protected and supported when they do.

It also includes ensuring that you act on these concerns. This will encourage employees to bring their concerns and breaches to management's attention, as well as being a way to protect and improve your organisation.

RECOMMENDATION 8

Focus on developing trust and psychological safety across your organisation. Create a culture where breach reporting is seen as a positive thing and support people who alert you to Code breaches and potential compliance issues.

PUT THE CONSUMER AT THE CENTRE OF YOUR BUSINESS

To behave fairly and honestly, insurers must hear the voice of the consumer. They must put themselves in the consumer's shoes and act accordingly.

RECOMMENDATION 9

Put the consumer at the centre of your thinking. Hear the consumer voice within your organisation. Ask what you can do to help your customers and create the best possible outcomes for them.

This recommendation helps you meet one of the purposes of the Code: to provide better outcomes for consumers and small business.

The following sub-recommendations will help you do this:

- Appoint a consumer advocate within your organisation who can be the voice of the consumer and who has enough power to influence culture, behaviours and business processes.
- Incorporate the consumer voice into operating models, product design, and reporting and governance frameworks. Make customer-centricity part of your business strategy so that customers' needs come before sales. Consider structuring your business so that it is organised around and focused on customers rather than on products.
- Treat consumer complaints as an opportunity to change practices and improve outcomes for consumers and small business. Complaints should not be ignored but should be taken as a sign of emerging risks or systemic issues. This includes:
  - complaints relating to the conduct of product distributors and service providers
  - complaints relating to other third parties engaged in carrying out services on your behalf (such as repairers)
  - complaints relating to the handling of complaints
  - external dispute resolution outcomes and definite systemic issues from AFCA.

The link between culture and remuneration

Culture and remuneration are intrinsically linked. As Commissioner Hayne pointed out in his Final Report on the Financial Services Royal Commission, the way an organisation's employees and directors are remunerated says much about that organisation's culture and sets the tone for how people are expected to behave:

> ***Remuneration and incentives, especially variable remuneration programs, tell staff what the entity rewards. Hence, remuneration and incentives tell staff what the entity values. Remuneration both affects and reflects culture … [P]oor remuneration and incentive programs can lead, and have led, to poor customer outcomes.***[12]

The Royal Commission was highly critical of the prevailing culture in the financial services industry of rewarding those who put the pursuit of profits ahead of legal obligations and good consumer outcomes. The insurance industry came under fire for misconduct over commissions, cold calling and the sale of add-on insurance – all of which generally form part of variable remuneration schemes, where staff are incentivised to hit sales targets rather than provide customers with appropriate products and services.

RECOMMENDATION 10

Make sure your measurement and reward systems do not focus solely on short-term profit. Do not reward behaviours that may be associated with unethical behaviour.

Structure your remuneration practices so that they align with your organisation's values. Make sure staff at all levels of the organisation are incentivised by and rewarded for desired behaviours and good consumer outcomes, with non-financial performance metrics given equal weight to financial performance metrics.

Put the interests of consumers and small businesses ahead of the financial interests of your salespeople and distributors. Your customers' needs should drive your processes, key performance indicators (KPIs), remuneration schemes and priority lists, which in turn helps ensure you offer the most suitable products and services.

RECOMMENDATION 11

Align your remuneration with consumer-centric cultural values. Reward desired behaviours and good outcomes for customers, not just profit. Include non-financial performance metrics and apply this at all levels of the organisation.

Five of the 76 recommendations put forward in the Final Report relate directly to remuneration and APRA responded swiftly, releasing a draft prudential standard (CPS 511 Remuneration[13]) which aims to clarify and strengthen remuneration requirements in APRA-regulated entities. The draft standard proposes requiring Boards to design a remuneration system that encourages the management of non-financial risks, reduces the use of financial metrics when determining variable remuneration, and improves information flow to the Board about risk management performance and its impact on remuneration.

[12] Financial Services Royal Commission Final Report, p. 335.

[13] Draft prudential standard CPS 511 Remuneration, APRA, July 2019.

The key reforms in the draft standard include the following:

- A proposed 50% cap on using financial performance measures in variable remuneration arrangements, meaning the remaining 50% must constitute non-financial performance measures.
- The need to demonstrate a link between an organisation's remuneration objectives, risk management framework (financial and non-financial) and performance measurement.
- Heightened oversight by the Board and/or remuneration committee for the overall remuneration framework, including the remuneration of the most senior employees.
- The need for organisations to provide APRA with more information about their remuneration practices so that APRA can better assess how they operate.

If you haven't already done so, you must review the way your staff are remunerated and incentivised so that you are able to meet the new standard when it is released.

RECOMMENDATION 12

Prepare now for APRA's proposed changes to CPS 511. Review how staff are incentivised and ensure non-financial performance measures are given equal weight to financial performance measures.

Using the Code as an ethical blueprint

The Code commits subscribers to openness, fairness and honesty in all dealings with consumers and small businesses.

You should use Commissioner Hayne's six principles as a lens through which to view the Code. This means you should not interpret the standards you commit to as a subscriber to the Code narrowly. You should be true to its purpose, which is to be open, fair and honest and provide high standards of service to consumers and small business. Take a broad view when interpreting the Code's standards, guided by the purpose and spirit of the Code, rather than seeking to limit their application or downplay their importance.

The Committee agrees with Commissioner Hayne that 'rules are merely a baseline; financial services industries should be trying to go much further to be fair, honest and transparent in their dealings with customers'.

It is worth noting that in a decision of the Full Federal Court in *ASIC v Westpac Securities Administration Limited*[14], the court identified 'fairness' as a new legal obligation. Westpac is appealing this judgement. However, insurers should take care to remember that, while being fair might not be captured exactly by the letter of every law, you are expected to treat it as a legal obligation.

More recently, the Federal Court found in *Delor Vue Apartments v Allianz Australia Ltd*[15], that Allianz had breached its duty of utmost good faith in the way it handled its customer's claim. Allianz was entitled to avoid the policy for non-disclosure but had told the insured it would not do so. It later went back on this and made a take it or leave it offer. The court found this conduct was 'unjust, unreasonable, unfair and did Allianz no credit as a commercial insurer by reference to expected standards of decent commercial behaviour'.

Use the Code as a tool to ask: 'Is this the best decision for the consumer?' When you are developing new products, making business decisions, creating strategies or plans, or undertaking any number of other organisational tasks, ask: 'are we actually doing what we say we'll do in the Code?' and 'are we acting in the best interests of consumers?'

[14] ASIC v Westpac Securities Administration Limited [2019] FCAFC 187

[15] Delor Vue Apartments CTS 39788 v Allianz Australia Insurance Ltd (No 2) [2020] FCA 588

RECOMMENDATION 13

Align the values of your organisation with the values in the Code. Then make sure norms and behaviours in your organisation align with those values.

While all sections of the Code are important to providing high standards of service, there are key sections that should be kept in mind when implementing and sustaining a positive culture. We have outlined below these key sections, taken from the new General Insurance Code of Practice 2020 (the new Code).

We will promote trust, integrity and respect by:

- ***meeting promises made to the community in a trusting environment;***
- ***being open, fair and understanding, and acting with integrity, our dealings with the community;***
- ***being clear, transparent, fair and timely in our communications with the community; and***
- ***treating the community with respect, dignity and sensitivity.***

This clearly sets out your obligation under the Code to be open, fair and honest. The Committee also encourages you to be transparent and ethical to reflect these values. The obligation in the Code specifically means you should interpret the Code broadly and not just obey the letter of the law. It is another reminder to ask 'what should we do?' rather than 'what can we do?'

Paragraph 21 of the new Code embraces the requirement to be open, fair and honest in all dealings with consumers:

21. We, our Distributors and our Service Suppliers will be honest, efficient, fair, transparent and timely in our dealings with you.

1. The objectives of the Code are:

a. to commit us to high standards of service;
b. to promote better, more informed relations between us and you;
c. to maintain and promote trust and confidence in the general insurance industry;
d. to provide fair and effective mechanisms for the resolution of Complaints you make about us; and
e. to promote continuous improvement of the general insurance industry through education and training.

The objectives of the Code should be the objectives of your organisation. Again, these relate to providing high levels of service and putting customer needs at the centre of your organisation.

2. We will pursue the above objectives of the Code with regard to the law and acknowledging that every contract of insurance is a contract based on the utmost good faith.

When you are dealing with a consumer or small business remember that good faith is as important as the letter of the law. This echoes Commissioner Hayne's requirement that financial services providers act fairly and interpret industry codes widely.
An ethical culture is seen in actions: goals, strategies and values are not enough. Make sure your actions reflect the Code. Keeping in mind the Code sections listed above will help you do this.

4. We acknowledge that our customers and our relationships with them are the foundations of our business.

This puts the consumers and small businesses that you serve at the centre of everything you do. You should consider them in all aspects of your business.

Ringing in cultural change

The findings of the Royal Commission have crystallised the need for subscribers to sharpen their focus on embedding a strong organisational culture that supports and values honesty, fairness and transparency. Some examples of how subscribers are changing and improving their approach to culture within their organisation in response to the Royal Commission's Final Report include the following:

- One subscriber has developed a Conduct and Culture Transformation Program, with the aim of delivering fair and suitable outcomes for customers, the community and the organisation.
- Another subscriber has commenced a program of work to refresh the culture and risk management frameworks within the organisation, with the aim of developing a consistent, future-focused and impactful culture narrative and a refreshed set of behaviours.
- Other subscribers have conducted staff engagement and risk culture surveys.

Subscribers are focusing on their customers as a way of bringing about cultural change and ensuring customers are receiving fair treatment and better outcomes. This is occurring in a number of different ways, including:

- Developing new practices (or enhancing existing practices) for identifying and responding to vulnerable consumers, including those experiencing financial hardship or family violence.
- Improving transparency, so that consumers have a better understanding of issues including policy coverage and their insurance needs; processes relating to sales, renewals and claims; and services provided by third parties.
- Creating a new 'Customer Experience Manager' role, with oversight of the Internal Dispute Resolution team and responsibility for ensuring that learnings from customer feedback and complaints result in better products and processes.
- Conducting complaints handling training for service providers.
- Rolling out complaints handling training via eLearning modules to all staff across the business.

Subscribers have also reviewed their remuneration frameworks in response to the Financial Services Royal Commission, putting in place a number of improvements to ensure that poor conduct is not rewarded. These include:

- Introducing risk and compliance outcomes in KPIs for executives, including the CEO.
- Reviewing remuneration systems for frontline staff and implementing commission caps.
- Introducing commission caps for the sale of on add-on insurance products.
- Making improvements to various incentive schemes, including for executives and those in risk and financial control roles, to ensure incentives align with activities that drive good customer outcomes.

In the words of one subscriber: "The entire organisation, from the Board down, is responsible for embedding and sustaining a healthy organisational culture."

Leadership and the Code: setting the cultural tone from the top

A customer-centric, Code-compliant culture cannot be successfully embedded within an organisation unless those at the top drive, support and model the desired behaviours and expectations. Leaders are responsible for advocating a Code-first approach and ensuring it cascades down through the business. They have ultimate oversight of compliance matters and must therefore be sufficiently informed to manage non-financial risk issues and challenge breach data.

The importance of 'walking the talk'

A strong organisational culture comes from strong and effective leadership – from leaders who are very clear in their expectation of how staff across the business should behave, particularly towards customers, and who role model that behaviour themselves. This applies not only to the executive team, who are generally more visible to staff on a day-to-day level; Board directors must also 'walk the talk' when it comes to the decisions they make and the tone they set for the rest of the business. Indeed, the first two principles of the Australian Institute of Company Directors' 10 Guiding Principles of Good Governance[16] speak directly to this obligation:

- Principle 1: The Board plays a key role in approving the vision, purpose and strategies of the organisation. It is accountable to the organisation's members as a whole and must act in the best interests of the organisation.
- Principle 2: The Board sets the cultural and ethical tone for the organisation.

BOARDS AND SENIOR EXECUTIVES MUST ADVOCATE A CODE-FIRST APPROACH

You cannot successfully embed a customer-centric, Code-compliant culture within an organisation unless those at the top drive, support and model the desired behaviours and expectations.

APRA's Prudential Inquiry into the CBA made clear the importance of setting the cultural tone at the top and ensuring it cascades down to all levels of the business:

> ***An important function of the Board is to set the tone within the organisation. This tone at the top is established through both internal and external communications, and demonstrated through the practical actions taken by the Board in its supervisory duties.***[17]

The tone coming out of your boardroom and C-suite must be one that advocates a Code-first approach throughout the organisation, where staff are incentivised by achieving good outcomes for customers and encouraged and emboldened to be proactive in identifying, managing and reporting breaches and incidents.

[16] Guiding Principles of Good Governance, Australian Institute of Company Directors, 2017.

[17] Prudential Inquiry into the Commonwealth Bank of Australia, APRA, May 2018, p. 13.

While the executive management, led by the CEO, plays a critical role in embedding those norms in a day-to-day, operational capacity, it is up to the Board to oversee how this occurs and to hold management to account for the outcomes. Delegating the management and implementation of culture to the CEO should not be a case of ‘set and forget’ for the Board. As Dr Sally Pitkin, a former non-executive director of the Australian Institute of Company Directors, points out:

> ***Although the duties of a non-executive director are critically different to those involved in the day-to-day management, non-executive directors cannot leave the issue of organisational culture entirely to management, because doing so fails to recognise the board’s leadership position. It also fails to recognise that the executive members of the leadership group will be living the culture and be enmeshed in it, and may not easily recognise dysfunction or sub-optimal aspects, or be willing or capable of challenging it.***[18]

As a company director, to achieve effective oversight of your organisation’s culture you need access to more information than simply what is provided in Board papers. You should ask to see the results of employee surveys, customer feedback, internal audit reports, reward and performance management procedures, and other performance metrics or operational dashboards that will allow you to compare outcomes with performance expectations.

BOARDS NEEDS TO SEE – AND BE SEEN BY – THE REST OF THE BUSINESS

In their APRA self-assessments, subscribers said engagement between the Board and the rest of the business needs to be improved to facilitate two-way communication and access a wider range of views on issues across the organisation.

As a Board member, you must be willing to ‘get out and about’ to see for yourself whether staff at all levels are conducting their duties in a way that aligns with your organisation’s cultural expectations and the key Code promises, and to demonstrate to staff that it’s imperative to you and your fellow Board members that they do so.

You can learn a lot about the cultural norms within your organisation by observing how your executive management team interacts with each other and with staff across the business, and by you and other Directors interacting with employees. Ideally, this should be done both in formal and informal settings, including Board meetings, company-wide Board presentations, site visits, training forums, call centre walk-arounds, and company events. Encourage two-way communication to give both Board members and employees the opportunity to raise any issues or concerns about Code compliance.

RECOMMENDATION 14

Invoke a culture of collaboration and unity by enabling Board members and executive management to regularly spend time with staff across the business. Let them watch how staff function on a day-to-day basis. Make it possible for them to listen in on customer calls across the entire value chain, including complaints. Encourage both parties to raise any issues or concerns about Code compliance.

EMPOWER YOUR STAFF TO DO THE RIGHT THING

As briefly mentioned in the ‘Culture’ chapter of this report, personnel right across the organisation need to feel psychologically safe speaking out about any processes or behaviours that could result in breaches of the Code, and to make decisions they feel are in the customer’s best interests. A psychologically safe workplace is one where staff are empowered to act without fear of punishment or reprisal, confident that what they say and do will be supported by those up the chain of command.

[18] Pitkin, S. The role of the board in corporate culture, Australian Institute of Company Directors, 2016.

Staff who feel psychologically safe will make decisions based on what is best for the customer, rather than relying on rigid processes, particularly when issues are not straightforward. They are also more inclined to take ownership of and learn from their mistakes.

Think about how psychologically safe your staff feel in to relation making customer-centric decisions that might be outside standard procedure. Are you confident that personnel right across your organisation would feel protected and supported if they expressed concerns or reported breaches and potential breaches of the Code? Are there clear processes for enabling this to happen? And are there documented procedures for following up and communicating the outcomes so that breaches can be learnt from and avoided in the future? If the answer to any of these questions is no or you are unsure, take action immediately – psychological safety is one of the central planks of a positive compliance culture.

Why the Board must be across all breaches of the Code

Leaders can't have effective oversight without all the facts – a point which was made by Commissioner Hayne in the Royal Commission Final Report:

> ***"Boards must have the right information in order to discharge their functions. In particular, Boards must have the right information in order to challenge management on important issues including issues about breaches of law and standards of conduct, and issues that may give rise to poor outcomes for customers."*** [19]

APRA's Information Paper on Self-Assessments of Governance, Accountability and Culture also highlighted this very real issue with its finding that there needs to be more rigorous Board and executive committee governance of non-financial risks[20].

All breach reporting – not just significant breach reporting – must extend to the most senior levels of an organisation. This includes the Board, Board Audit and Risk Committee and executive management. You at the top are responsible for the strategy and direction of the organisation but you are also responsible for ensuring everyone in the organisation is complying with the Code and doing the right thing by the consumer.

Without a complete picture of emerging issues on risk and compliance, and customer complaint trends, you are effectively 'leading blind', unable to assess the need for – and drive – change, and unable to support frontline staff to improve processes, remediate breaches and prevent them from recurring.

HOW DO SUBSCRIBERS REPORT BREACHES TO THEIR BOARDS?

Some subscribers reported that their Board actively reviews and analyses breach data. For example, one subscriber's Board discusses breaches and, crucially, their remediation with the Manager of Compliance and Risk and the CEO, as well as discussing any breach trends. Another subscriber noted that breaches and incidents are both reported to the Board formally and discussed less formally through an open line of communication between management, the Board and the Board's Audit and Risk Committee.

A subscriber's size and resourcing appear to play a role in how breaches and significant breaches are reported to Boards and executive management.

Some smaller subscribers reported that their Boards do not examine breach data. In some cases, this was because the subscriber was a branch of a foreign insurer, or because the subscriber did not have a decision-making Board. In the Committee's view, size and/or foreign ownership are not excuses for a lack of oversight by a subscriber's Board or senior decision-makers. We expect all subscribers to alert their leadership personnel to breaches of the Code, and for Boards to actively examine breach data to identify trends, understand root causes and outline their expectations for corrective and preventive action.

[19] Financial Services Royal Commission Final Report,p. 400.

[20] Information Paper: Self-assessments of governance, accountability and culture, APRA, May 2019.

For other smaller subscribers with fewer layers, breaches are typically seen earlier by executive management and Boards, and senior managers are more involved in the end-to-end breach process. Many of these smaller subscribers said that they report significant breaches to the Board and/or to executive management as soon as it is identified as a significant breach, rather than waiting to report it in the formal reporting cycle.

This is good practice, as it gives Boards early visibility of breach issues and trends and helps to ensure that subscribers are able to meet their obligation to report significant breaches to the Committee within 10 business days. The Committee acknowledges that it may be more difficult for larger organisations to implement but we encourage all subscribers to consider monthly meetings or providing additional informal communication to their Boards, instead of relying solely on quarterly meetings.

AN EXAMPLE OF GOOD PRACTICE

One subscriber's Chief Risk Officer has a direct reporting line to the Board (through its delegated Board Risk Committee) and escalates incidents raised during the Incident and Breach Reporting Forum to the Executive Committee as necessary. As such, Executive Management and the Board have full transparency of the breach reporting and customer rectification process.

THE ROLE OF BOARD AUDIT AND RISK COMMITTEES

All larger subscribers reported that their Boards have Board Audit and Risk Committees or forums to which significant breaches (and in some cases, all breaches) are reported. Board Audit and Risk Committees have oversight of risk and compliance and the processes for identifying, evaluating and managing risk. Typically, the compliance function is responsible for reporting breaches and significant breaches to the Board Audit and Risk Committee.

There was variability in the nature and comprehensiveness of breach reporting to Board Audit and Risk Committees. At the most comprehensive end, one subscriber described a suite of reports including a group compliance report, quarterly risk report, management committee report and a weekly breach report. Other subscribers referred to a single compliance update or report including information on breaches and compliance incidents. Some of the larger subscribers also referred to automated reporting coming out of their breach register system, a potentially useful source of real-time information.

RECOMMENDATION 15

Report all breaches to the Board, not just significant breaches. Report at least monthly and allow for significant breaches to be reported as they happen. Give Boards access to online breach registers so they can extract reports in real time.

BOARDS MUST CHALLENGE BREACH DATA

In its October 2019 report, 'Director and officer oversight of non-financial risk'[21], ASIC's Corporate Governance Taskforce strongly advocates for Boards to examine closely and challenge all the information reported to them by senior executives about non-financial risk, citing the following as evidence of active oversight by Board directors:

- Requesting further information, analysis or action from management.
- Asking questions of management.
- Requesting changes to recommendations or proposals.
- Rejecting recommendations or proposals.
- Driving the implementation of changes to address identified failures by management.

[21] REP 631 – Director and officer oversight of non-financial risk report, Corporate Governance Taskforce, ASIC, October 2019.

The Committee concurs with ASIC on this matter. Breach reporting must not be viewed as a one-way conversation. Boards must actively review and analyse the information they receive about Code breaches in order to understand why they occurred; to assess the merits of the proposed remediation; and to hold management to account for preventing similar breaches in the future. This applies to all Code breaches, not just significant breaches.

The Committee's role in guiding effective leadership and Code compliance

One of the functions of the Code Governance Committee is to provide Code subscribers with guidance on how to comply with the Code. Publications like this one give Boards, senior leadership teams and delegated risk committees insight into industry trends and issues, along with recommendations for achieving best practice in their Code compliance.

The Committee expects its reports and recommendations to be distributed to all levels within subscribers' organisations, including their Boards – an expectation that was reiterated by the Committee in two of the reports published during 2019 (*How insurers handle consumer complaints and General Insurance in Australia 2017–18*). It is evident from subscribers' responses to this inquiry that this is not happening. In its recently released (April 2020) *Annual Report 2018-19* the Committee said that it expects subscribers to distribute the report to all levels within their organisations, including their Board of Directors and Executive Management.

Just six of the 45 subscribers who took part in this inquiry said they provided some of the Committee's publications directly to their Boards and even then, most could not specify which publications their Boards had seen. A further eight subscribers said they relied on management to provide key updates and summaries to their Boards and/ or risk management committees, while six said they circulated relevant publications at an operational level through their senior leadership/executive management teams and/or their compliance areas.

Some larger subscribers reported that senior leaders provide their risk management committees with summaries or updates of the Code Governance Committee's publications. This is acceptable practice, provided that:

- there is a direct reporting line between the Board and its risk committee, or where the risk committee is a Board sub-committee
- the summaries or updates provided to the risk committee highlight the issues, risks and recommendations specified in the CGC's publications
- the risk committee is empowered to direct and enact the recommendations made in the Committee's publications.

Best practice is to table all Committee reports at a Board or Board sub-committee level, with a summary of the key findings, observations and recommendations to improve Code compliance. Board members should also be made aware of any specific implications and recommendations for the organisation, along with a copy of or hyperlink to the full report.

For their part, Boards and Board risk committees must assign responsibility for implementing the Committee's recommendations to the appropriate business area and take appropriate steps to monitor the outcome through clear reporting lines.

RECOMMENDATION 16

Alert your Board or delegated sub-committee to the Code Governance Committee's publications. Highlight key findings, observations and recommendations and explain how these are relevant to your business and its Code compliance obligations.

The keys to good governance: processes, people and resources

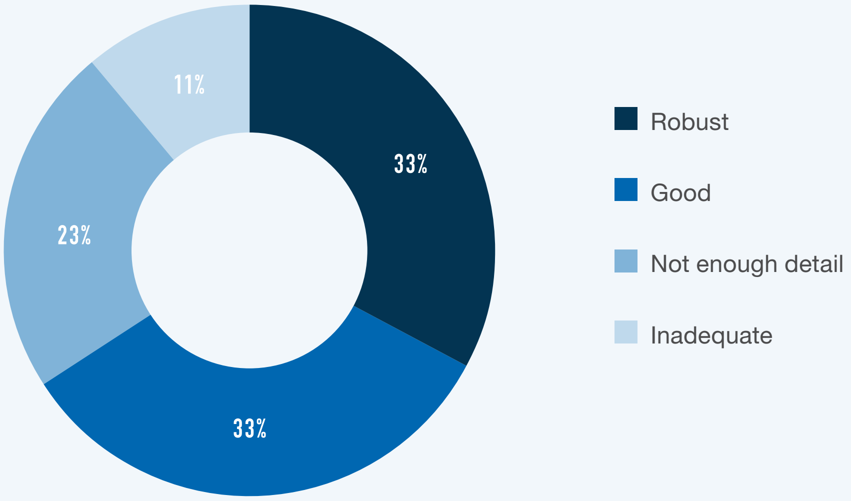
Corporate governance is the framework of systems, processes and procedures in place to control, monitor, guide and direct an organisation. It underpins the judgement and behaviour of those throughout the business but especially those at Board and executive level. Sound governance frameworks lead to effective oversight and management of risk and help instil a culture of accountability within an organisation – one where people are expected to take ownership of risk, including non-financial risk, and encouraged to deliver sound outcomes.

Why you need a robust compliance framework

An effective compliance framework is a vital mechanism for supporting people within an organisation to understand and abide by their Code obligations, recognise when Code breaches occur and report them in a timely fashion.

A robust compliance framework incorporates the right risk management model – one with clearly understood roles and accountabilities. It is supported by making your staff and third-party distributors aware of their obligations under the Code of Practice, providing them with the right competencies and training, regularly monitoring them, and ensuring that effective processes and procedures are in place to facilitate timely identification and reporting of breaches. To achieve this, compliance must be taken seriously in the organisation and supported by investment in suitable resources.

FIGURE 4: SUBSCRIBERS' COMPLIANCE FRAMEWORKS



As part of the own motion inquiry, subscribers were asked a series of questions about their compliance frameworks, the controls and internal reporting they include, and how they are reviewed (see questionnaire in Appendix 1). Around one-third (33%) of subscribers described a robust compliance framework that meets Committee expectations. These subscribers described comprehensive frameworks adhering closely to the three lines of defence model and were seen as examples of best practice. Another third (33%) described compliance frameworks with some of the elements of a best practice framework, but room to improve. Of the remainder, around 11% described a framework that needs considerable improvement, while around 23% did not describe their compliance framework in enough detail.

Some subscribers are taking steps to enhance their compliance frameworks, investing in compliance roles, improving reporting systems and building Code awareness and a culture of self-reporting. Others need to take urgent action to improve their compliance frameworks, enacting the recommendations outlined in this chapter at a minimum.

RISK GOVERNANCE: THE THREE LINES OF DEFENCE MODEL

The three lines of defence model is widely acknowledged as the backbone of a robust risk management framework. It is the preferred risk governance model for all APRA-regulated institutions as it supports compliance with APRA's Prudential Standard CPS 220 Risk Management[22].

The model's purpose is to help you provide a coordinated approach to risk and assurance by assigning roles and responsibilities across three separate, independent levels within your organisation, where Executive Management and the Board sit outside the model but have ultimate oversight of all three lines (see Figure 5).

FIGURE 5: THE THREE LINES OF DEFENCE MODEL

BOARD

- Establishes a governance structure (board sub-committees, executive responsibilities and risk management and assurance functions).
- Is ultimately responsible for the risk management framework and oversees its operation by management.
- Sets the risk appetite within which it expects management to operate and approves the risk appetite statement.
- Approves the institution's risk management strategy.
- Forms a view of the risk culture in the institution, and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite, identifies any desirable changes to the risk culture and ensures the institution takes steps to address those changes.

Board Risk Committee

Board Audit Committee

1ST LINE OF DEFENCE
Risk owners

BUSINESS MANAGEMENT

Implementation, ongoing maintenance and enhancement of the risk management framework, including:

- identification and effective management/mitigation of risks; and
- issues identification, recording, escalation and management.

Likely to include executive and management committees, forums and delegated authority.

2ND LINE OF DEFENCE
Review and challenge

RISK MANAGEMENT AND COMPLIANCE FUNCTION(S)

Independent oversight of the risk profile and risk management framework, including:

- effective challenge to activities and decisions that materially effect the institution's risk profile;
- assistance in developing, maintaining and enhancing the risk management framework; and
- independently reporting lines to appropriately escalate issues.

3RD LINE OF DEFENCE
Independent assurance

INTERNAL AUDIT FUNCTION /3RD PARTY

At least annually, independent assurance that the risk management framework has been complied with and is operating effectively.

At least every three years, a comprehensive review of the appropriateness, effectiveness and adequacy of the risk management framework.

[22] APRA Prudential Standard CPS 220 Risk Management

HOW ARE SUBSCRIBERS IMPLEMENTING A THREE LINES OF DEFENCE MODEL?

While not all subscribers have a three lines of defence model in place, most acknowledged the importance of the model, and recognised the need to enhance and embed it within their organisations. In the initial survey for the own motion inquiry, 12 subscribers explicitly stated that they use a three lines of defence model, as did all 10 of the subscribers who responded to the follow-up questionnaire about the effectiveness of their compliance frameworks[23].

The **first line** of defence refers to the frontline functions such as sales, underwriting, claims and dispute resolution that own and manage risk, largely with a real-time focus. Subscribers considered the first line to have primary accountability for complying with obligations, including Code requirements, by following organisational frameworks and policies, implementing and monitoring controls, conducting quality assurance and identifying and reporting incidents and breaches.

The **second line** refers to functions that oversee risk or specialise in risk management and compliance (such as Governance, Risk and Compliance teams) and are responsible for effective compliance and risk frameworks. The role of the second line function includes supporting the Board and relevant delegated committees by developing risk management policies, systems and processes to facilitate a consistent approach to identifying, assessing and managing risks. It also provides specialist advice and training on risk-related matters to the Board, Board committees and the other lines of defence.

Among subscribers, there was variation in the scope and functions of the second line, which could include any or all of:

- assessing risk appetite and exposure
- developing compliance monitoring plans
- providing compliance advice to the first line
- monitoring and reviewing breaches and incidents and how they are reported and remediated
- overseeing external dispute resolution
- developing and continuously improving the compliance framework
- managing external breach reporting and relations with regulators.

Some subscribers embed risk and compliance professionals within the first line, in addition to maintaining a discrete second line function, while others have a sharper division between the first and second lines.

The third line refers to audit functions that provide independent assurance to Executive Management and the Board, evaluating the adequacy and effectiveness of both first- and second-line risk management. Some subscribers referred to both internal and external auditing, while others appeared to rely on internal auditing only.

However, most subscribers had less structured frameworks that featured some but not all of the same elements as those based on the three lines of defence model. Those elements include:

- documented policies, processes and procedures that provide guidance to staff
- a Compliance Plan documenting the obligations relevant to different roles
- a Risk Appetite Statement setting out the amount and type of risk that the subscriber is willing to take on in order to meet its strategic objectives
- an Incident and Breach Management process or policy, together with a system for recording and managing incidents and breaches
- a Risk and Compliance Committee or forum that meets regularly.

THE NEED FOR CLEARER ROLES AND GREATER ACCOUNTABILITY

For a three lines of defence model to work effectively, each line function must clearly understand what its responsibilities are, to whom it's accountable, and how its role fits into the organisation's overall risk and control framework. Members of all three lines need to meet regularly to discuss compliance and risk issues, to ensure each is aware of their obligations and to prevent duplication of efforts.

Several subscribers acknowledged that a lack of clarity between the roles and responsibilities of each line function is causing weaknesses in their three lines of defence, with many recognising that Line 1 staff are overly reliant on the

[23] Some of these subscribers advised that they operate a three lines of defence model when responding to the first survey.

second-line function as a safety net for controlling risk, and that Line 1 staff need to take greater ownership of identifying and managing risk.

The absence of the Line 3 audit function is also an issue for some subscribers. Without an independent reporting mechanism providing the Board and Executive Management with assurance that risk management is working effectively, there is a very real danger that breach reporting will not escalate beyond the level of Line 2. Indeed, this may explain why there are low levels of breach reporting to the Committee. If the Board is not made aware of breaches, governance is not effective, breaches can't be remediated, learnt from and prevented from happening again, and they won't be reported to the Committee.

If there is no dedicated Line 3 function in your organisation, you should implement one as a matter of priority. Two lines of defence is not enough for effective risk management.

BETTER RESOURCING ACROSS ALL THREE LINES OF DEFENCE

Some subscribers conceded that their Line 2 functions should be better resourced, with more compliance staff and improved risk-management systems and processes in place. As an example, one subscriber reported that risk profile data is captured in spreadsheets maintained by Line 2, limiting the ability to perform risk analysis and deliver more meaningful stakeholder reporting. This is consistent with the outcomes of APRA's self-assessment report, which found that non-financial risk management frameworks are less visible than financial risk management frameworks in most institutions, leading to a lack of investment in resources for compliance functions. There is further analysis of this in the 'Investing in Compliance' section on page 37.

RECOMMENDATION 17

Include a robust three lines of defence model in your risk management framework that is actively championed by the Board. Always include the third line function, no matter how small your organisation. Clearly define each line function's roles and accountabilities so that individuals understand their responsibilities, and facilitate regular meetings between lines to reinforce this.

Controls, systems and processes

CONTROLS

You must have controls in place to make sure breaches are prevented where possible, and otherwise detected, recorded, reported, addressed and remedied appropriately. Controls should be both documented and embedded in processes and practices.

Some of the controls subscribers described as having in place include:

- automated reports and alerts built into processes and systems
- quality assurance monitoring, such as file reviews
- breach and incident reporting by staff, with review by the first and sometimes second line
- training and coaching, both proactive and in response to incidents and breaches
- compliance obligations built into contracts with distributors and service suppliers
- compliance attestations.

In many cases, subscribers' descriptions of their controls were not detailed enough for the Committee to be confident that they are capable of detecting, let alone preventing Code breaches. Smaller organisations and teams tended to have less formal control arrangements – for example, some subscribers described relying on a single manager or staff member for some functions, and said they used manual control systems and processes.

The Committee regards this as inadequate, as the margin for error is too great. You should automate controls wherever possible so that alerts for incidents and breaches occur automatically, systems have built-in triggers for Code requirements relating to timeframes, and reliance on manual intervention is minimal.

RECOMMENDATION 18

Automate controls so that breach alerts and reporting do not rely on manual intervention. Have systems with built-in triggers for Code requirements relating to timeframes.

Positively, some subscribers described processes for reviewing or testing the controls that are in place. One subscriber described an annual control testing program that provides for review of the design and operating effectiveness of controls. Another subscriber noted that Risk and Compliance Officers embedded in the first line have a role overseeing the effectiveness of process controls.

REPORTING SYSTEMS

Some subscribers are increasing their focus on robust reporting. This is being done in a range of ways, including by:

- updating systems - for example, by moving from an Excel breach register to an Enterprise Risk Management System
- thoroughly documenting the incident management framework
- redesigning incident management forms to improve quality of reporting data
- implementing regular reviews to check for and investigate any spikes in Code breaches
- creating a formalised monthly incident and breach forum to improve awareness, identification and reporting.

GOOD PRACTICE EXAMPLE OF AN INTEGRATED RISK ISSUE AND INCIDENT SYSTEM:

One subscriber has implemented an organisation-wide integrated risk issue and incident system to record and report on incidents, issues and potential breaches of the Code, laws, regulations, external contractual arrangements and internal policies.

Using the system, all employees are required to identify and record incidents within five days so that the causes and consequences can be examined and reviewed through the Breach Management Process. The system delegates ownership of incidents and breaches to executive management to ensure that breaches are reported appropriately.

Weekly Code breach reports are provided to executive management by Line 2 compliance advisory staff, and include a request for further information and an outcome of the breach assessment. Where breaches may be significant and/or reportable, a Breach Committee (consisting of compliance advisory staff, the relevant executive manager and business area staff) is convened to discuss the root cause, remediation and the prevention of future breaches.

CONTINUOUS IMPROVEMENT

Some subscribers reported that they monitor their compliance frameworks continuously, with processes and systems updated as required. For example, one subscriber has implemented a forum of senior managers from legal, risk, operational, compliance and claims areas to meet every six weeks, addressing as a standing item the Code Governance Framework, breaches and any systemic issues. This is a good way to remain proactive and abreast of current issues. Defined projects with set timelines are also useful for letting you plan improvements to compliance frameworks and make sure they occur in a timely manner.

Some larger subscribers reported on detailed projects that are underway to review or make changes to compliance frameworks and were able to give estimated completion dates. Other subscribers described strategies detailing key activities over an 18 to 24 month period.

CODE COMPETENCY FOR STAFF

In a sign that more needs to be done to improve Code awareness and competency among staff, many subscribers – even those with apparently comprehensive compliance frameworks – are reporting surprisingly low numbers of breaches to the Committee.

Code compliance is ultimately driven by behaviour, not by a framework. You can have a comprehensive compliance framework in place, with a leadership team that advocates and espouses a Code-first culture, but these mean nothing if your staff don't understand the Code's purpose, their obligations to comply with it and the importance of breach reporting.

Training in Code compliance has an important role to play, as discussed below. However, improving Code awareness and staff competency can't be achieved through training alone. Rather, it comes from embedding an ethical, consumer-focused culture as described in earlier chapters of this report, where:

- Code compliance is demonstrably 'lived' through the decisions and actions of staff at all levels
- fairness, honesty and transparency are valued above all else
- customers' best interests are placed at the centre of all decision-making
- staff are encouraged to report Code breaches as they occur.

HOW CAN YOU ENSURE CODE COMPETENCE AMONG YOUR STAFF?

Asked how they ensure the competence of their employees to identify and report compliance incidents and Code breaches, subscribers said they provide formal and informal training that is supported by a range of policies, systems and procedures.

Formal training includes mandatory Code training for employees at induction, and periodic refresher training. Refresher training is often via an online e-learning module. Informal (or less formal) training includes activities such as coaching, reinforcement, oversight, support, and QA programs. These activities are generally conducted by team leaders and management, Line 1 risk and compliance officers and the Line 2 compliance function.

Most subscribers provide their employees with training around awareness of the Code and Code obligations. However, few provide specific training on how to report incidents and Code breaches, and even fewer conduct targeted Code training for specific groups of employees, such as sales staff or claims assessors, as opposed to generic Code training for all employees.

The types of processes and procedures subscribers have in place to support their Code compliance training include online incident management systems that enable staff to report incidents and breaches, and documented policies and guidelines with step-by-step instructions for them to follow when doing so.

To achieve full Code competency across your workforce, your Code compliance training program should consist of educating all staff about the Code – including its role in the consumer-protection framework, your organisation's obligations as a Code subscriber, and how the Code underpins the cultural and behavioural expectations of everyone who works in your organisation – as well as how to report and manage incidents and breaches.

This should extend to all personnel, not just front-line staff. Areas such as product creation, marketing, IT and project management can be the cause of incidents and breaches. In 2018–19, for example, we saw subscribers report a number of significant breaches caused by incorrect or misleading information about insurance products being published on their websites. The need to take the Code seriously must be made clear right across the organisation.

AN EXAMPLE OF GOOD PRACTICE

All employees of one particular subscriber are required to undertake mandatory compliance training annually to ensure awareness and understanding of applicable compliance obligations. Training includes breach management, a module on Code obligations to ensure awareness of the Code in all staff, a module on the incident reporting process and responsibilities, and the importance of incident reporting.

Run formal Code training as part of the induction process for new staff and follow it up with 'refresher' training at least once a year to remind all staff of their Code obligations. This should be more rigorous than a 'set and forget' self-guided e-learning module.

Provide bespoke Code training to specific areas of the business, particularly those who deal most closely with customers, such as sales, claims and complaints teams. One subscriber reported that efforts to build a self-reporting culture in the claims function, including through the introduction of claim self-audits, was leading to an increase in self-reported incidents and breaches.

RECOMMENDATION 19

Embed a consumer-centric culture where staff understand the values of the Code and their obligations to consumers. Explain why and how they must report breaches. Do this when onboarding new staff and follow it up with regular 'refresher' training. Assess the effectiveness of your staff training and monitor the outcomes for any gaps or deficiencies.

Your training should be reinforced with policies that outline employees' Code compliance responsibilities and accountabilities, and sufficiently detailed process documents with the steps they need to follow when reporting incidents and breaches.

You should also issue regular communication from senior management (including the Board), team leaders and the compliance function that promotes a Code-first approach and encourages staff to flag compliance issues and breaches. This could be via staff e-newsletters and intranet articles, as well as team meetings. As an example, one subscriber described a recent targeted communication initiative on breach reporting, alongside the development of 'bite sized' communications to be rolled out across the internal social media platform.

RECOMMENDATION 20

Make it easy for staff to report incidents and Code breaches. Encourage them to see breach reporting as a good thing – a chance to 'right a wrong' and prevent it from happening again.

THE TRAINING–BREACH CONUNDRUM

Despite reassuring the Committee over the last five years that they are providing excellent Code competency to their employees, subscribers consistently attribute many breaches to people-related causes such as inadequate staff training, human error and a failure to follow the correct processes and procedures. For example, when subscribers are asked to explain the reasons for breaches of the Code's buying insurance standards, many point to poor practices by sales staff when selling insurance products to consumers.

As a consequence, the Committee has serious questions to ask about the effectiveness of subscribers' Code competency programs. Is the compliance training being rolled out to staff ineffective or focused on the wrong things? Are the outcomes being reviewed and appropriately measured against Code compliance? Is training merely seen as a box-ticking exercise rather than an opportunity for meaningful learning?

If your organisation has recorded a high number of breaches with people-related issues as the root cause, you must assess the efficacy of your Code compliance training. The advent of the new 2020 Code of Practice provides a golden opportunity to conduct a 'root and branch' review of your Code competency programs to ensure they advocate a culture where the Code is 'lived' by all employees.

Code competency for distributors

Both the 2014 Code and the new 2020 Code require subscribers to ensure that their distributors – those who sell insurance products on the subscriber's behalf – are appropriately educated and trained on the Code and their compliance obligations. As we saw during the Royal Commission, however, misconduct relating to commissions, cold calling and the sale of add-on insurance indicates that better oversight and management of third-party distributors is needed.

HOW CAN YOU ENSURE CODE COMPETENCE AMONG YOUR DISTRIBUTORS?

Subscribers use a mixture of training, monitoring and contractual obligations to ensure their product distributors and service suppliers identify and report incidents and Code breaches to them in a timely way. The majority require their distributors to undergo Code training (most often provided by the subscriber in the form of an online Code training module or similar) so that they are aware of the Code's purpose and their compliance obligations. Code compliance for distributors should be normalised behaviour and not motivated by inappropriate incentives.

Around half of subscribers said they have arrangements in place to monitor and support their distributors to comply with their Code obligations, with arrangements including attestations from distributors, and performance reviews and audits of distributors' operations. In one case, a subscriber reported that it has three dedicated managers who liaise with partner organisations to provide monitoring and support.

Some subscribers include specific clauses in their contracts/service level agreements (SLAs) with distributors, stipulating that the distributors must comply with the Code, and in some cases, report all incidents and breaches to the subscriber.

Interestingly, only one of the surveyed subscribers reported that they have in place all three methods of oversight mentioned above to ensure Code compliance by their distributors – an approach the Committee considers best practice.

Review the contracts/SLAs you have with your distributors to make sure they include clauses that not only require them to comply with the Code but also require them to report any incidents or breaches to you within one business day. Specify that your distributors must undertake training both in the Code's standards and in how to identify and report Code breaches, and if you are not providing that training to your distributors, make it a requirement that your distributors provide you with evidence that Code training has been carried out. Implement appropriate monitoring arrangements that give you sufficient oversight of your distributors' operations and carry out regular reviews and audits to ensure they are identifying and reporting breaches to you in a timely manner.

RECOMMENDATION 21

Ensure your distributors and service suppliers are fully aware of the Code and their compliance obligations. Check that they know how to identify and report breaches and potential breaches of the Code. Include clauses in their contracts/service level agreements that require this and stipulate the consequences for non-compliance.

Investing in compliance

The APRA self-assessments paper reported that many institutions, particularly in banking and insurance, acknowledged that their organisation's risk and compliance functions should be given greater status and influence. In his Final Report, Commissioner Hayne also made reference to some financial services entities failing to give compliance staff a strong enough voice in the business, and devoting inadequate resources to compliance.

Addressing these issues requires investment in compliance and risk management, to achieve outcomes including:

- increased staff numbers and improved capabilities within compliance functions of the business
- elevated seniority of some risk and compliance roles to a level sufficient to challenge management
- enhanced reporting systems and processes for managing operational and compliance risk – including those relating to quality assurance, internal audit and complaints handling.

Some subscribers are demonstrably investing more in compliance and risk areas. One way in which they are doing this is by resourcing new compliance roles. For example, in 2018, one subscriber increased its compliance team from two to six full time employees. At the same time, it created new positions in the claims function for workplace capability consultants, who provide expert advice and guidance on all aspects of compliance, quality assurance and quality improvement within the first line claims function. They are also responsible for identifying, designing and implementing key capability development, training and coaching initiatives. Similarly, another subscriber described a new initiative to embed a specific compliance role within the first line claims function.

RECOMMENDATION 22

Invest in compliance-specific staff. Make it their job to conduct comprehensive compliance assurance reviews to identify legislative, regulatory and Code non-compliance.

Glossary

Defined terms from the Code

Authorised representative means a person, company or other entity authorised by **us** to provide financial services on **our** behalf under **our** AFS licence, in accordance with the Corporations Act 2001.

Code means the General Insurance Code of Practice 2014.

Complaint means an expression of dissatisfaction made to **us**, related to **our** products or services, or **our Complaints** handling process itself, where a response or resolution is explicitly or implicitly expected.

Employee means a person employed by **us** or by a related entity that provides services to which this **Code** applies.

Insured means a person, company or entity seeking to hold or holding a general insurance product covered by this **Code**, but excludes a **Third Party Beneficiary**.

Retail Insurance means a general insurance product that is provided to, or to be provided to, an individual or for use in connection with a **Small Business**, and is one of the following types:

a) a motor vehicle insurance product (Regulation 7.1.11);

b) a home building insurance product (Regulation 7.1.12);

c) a home contents insurance product (Regulation 7.1.13);

d) a sickness and accident insurance product (Regulation 7.1.14);

e) a consumer credit insurance product (Regulation 7.1.15);

f) a travel insurance product (Regulation 7.1.16); or

g) a personal and domestic property insurance product (Regulation 7.1.17),

as defined in the Corporations Act 2001 and the relevant Regulations.

Small Business means a business that employs:

a) less than 100 people, if the business is or includes the manufacture of goods; or

b) otherwise, less than 20 people.

we, **us** or **our** means the organisation that has adopted this **Code**.

you or **your** means an **Insured** or **Third Party Beneficiary**, or as otherwise stated in relation to a particular section of this **Code**.

Appendix 1. Questionnaires

Questionnaire 1

In October 2018, the Committee sent a letter with its initial questionnaire to the CEOs of 45 Code subscribers.

A 'targeted' questionnaire was sent to 26 subscribers (which included 15 coverholders and claims administrators) and a 'generic' questionnaire was sent to 19 subscribers.

TARGETED QUESTIONNAIRE

Years to analyse:

A) 2014-15

B) 2015-16

C) 2016-17

D) 2017-18

E) Year to date from 1 July 2018 – only in relation to significant breaches.

1. Analyse the number of breaches reported by your company in the Annual Industry Data Report for each of the years listed above.
   Explain the variations between each year and if applicable:

   a) why in some years the breach numbers were the same as the year before and/or

   b) why your company did not report any breaches in a year or years?

2. Review the number of significant breaches reported by your company in each year and explain:

   a) if any significant breaches of the Code were not reported, why not?

   b) are the frameworks used to identify and report significant breaches sufficient and if so, why do you believe they are?

With respect to the processes and systems used to monitor compliance and report Code breaches (frameworks):

3. Describe the frameworks that are currently in place.

4. Tell us what controls are used to ensure that the frameworks used are effective and that breach data is:
    a) recorded and reported properly, and
    b) addressed appropriately.

5. What types of audits are done to assess the adequacy and effectiveness of compliance monitoring frameworks?

6. What work is being done to improve the strength of the current frameworks and address deficiencies?

7. What are the timeframes to set up and implement new or improved frameworks?

8. Are you, your Board and executive management confident that you have accurately reported significant breaches to the Committee over the last 4 years and from 1 July 2018 year to date?

9. Describe how breaches of the Code, especially significant breaches, are reported at Board and executive management level.

10. What steps are taken at Board and executive management levels to:
    a) ensure the accurate reporting of breaches to the Code Governance Committee occurs, and
    b) that they are sufficiently addressed taking into consideration the full scale and impact of any consumer detriment.

11. If the processes and frameworks to report Code breaches to the Board and executive management do not exist or are deficient, explain what is being done to address this?

12. Would your company be willing to share the outcomes and findings of the APRA self-assessment review with the Committee on a confidential basis? If so, please provide a copy.

GENERIC QUESTIONNAIRE

Years to analyse:

F) 2014-15

G) 2015-16

H) 2016-17

I) 2017-18

1. Analyse the number of breaches reported by your company in the Annual Industry Data Report for each of the years listed above and explain the variations between each year.

2. Review the number of significant breaches reported by your company in each year and explain:

   c) if significant breaches of the Code were not identified why?

   d) are the frameworks used to identify and report significant breaches sufficient and if so, why do you believe they are?

With respect to the processes and systems used to monitor compliance and report Code breaches (frameworks):

3. Describe the frameworks that are currently in place.

4. Tell us what controls are used to ensure that the frameworks used are effective and that breach data is:

   c) recorded and reported properly, and

   d) addressed appropriately.

5. What types of audits are done to assess the adequacy and effectiveness of compliance monitoring frameworks?

6. What work is being done to improve the strength of the current frameworks and address deficiencies?

7. What are the timeframes to set up and implement new or improved frameworks?

8. Does your Board examine your breach data and consider whether breaches have been appropriately addressed?

9. Would your company be willing to share the outcomes and findings of the APRA self-assessment review with the Committee on a confidential basis? If so, please provide a copy.

Questionnaire 2

In March 2019, the Committee sent a letter to the Board Chairs of the 45 Code subscribers participating in the inquiry.

That letter asked the following questions:

As a follow-up to my letter of 5 October 2018 and if applicable, by the end of March 2019 please provide:

- a copy of your organisation's APRA self-assessment (or similar review) and outcomes, if it has not already done so, and/or
- any further information to expand or clarify your organisation's initial response.

Further, the Committee would appreciate advice by the end of March 2019 as to which of the Committee's reports, audits and inquiries have been submitted to your board for consideration and action as appropriate, since July 2014 when the new Code commenced. A full list of the Committee's reports is included below.

Title of Code Governance Committee publication	Date of release
2012 General Insurance Code of Practice, Aggregated Industry Data Report, Overview of the Year 2013–2014	March 2015
2012 General Insurance Code of Practice, Annual Report 2014–2015	October 2015
The General Insurance Industry Data Report 2014–2015, 2012 General Insurance Code of Practice	June 2016
General Insurance Code of Practice, Annual Report 2015–2016	September 2016
General Insurance Code of Practice Industry Data Report 2015–16	March 2017
2014 General Insurance Code of Practice	
Own Motion Inquiry, Investigation of Claims and Outsourced Services	May 2017
General insurance in Australia 2016–17, Industry practice and Code compliance	March 2018
Guidance note no. 1, Financial hardship obligations –	
General Insurance Code of Practice	March 2018
Who is selling insurance? 2014 General Insurance Code of Practice, Own Motion Inquiry	June 2018
How insurers handle consumer complaints, 2014 General Insurance Code of Practice, Desktop Audit	January 2019

Questionnaire 3

In August 2019, the Committee sent a third letter to the CEOs of ten selected subscribers with a further questionnaire as follows:

1. Is there any conduct that your organisation considers is not subject to the Code's standards? If yes, please provide your reasons and describe the relevant conduct.

2. How does your organisation ensure the competence of its employees to identify and report compliance incidents and breaches that could potentially breach the Code?

3. What factors does your organisation consider when assessing whether conduct has breached the Code?

4. If your organisation has reported a higher number of Code breaches in its annual data return for the year ending 30 June 2019 than it has compared to 2017–18:

   a) What was the total number of Code breaches that it reported for 2018–19?

   b) What are the factors that contributed to the increase in reported breaches?

5. What is your organisation's understanding of the operation of 'significant breach' as defined by the Code?

6. How does your organisation apply the criteria that define a significant breach when assessing whether conduct has significantly breached the Code?

7. How does your organisation ensure that its product distributors and service suppliers identify incidents that could potentially breach the Code and notify it of these in a timely way?

8. Does your organisation consider that it has a robust approach to root cause analysis of breaches and significant breaches? Describe your organisation's approach to root cause analysis including strengths, weaknesses and any improvements it plans to make.

9. Does your organisation review, or it would it review, the following against the Code's significant breach criteria?

   a) A definite systemic issue identified by AFCA.

   b) A significant breach identified by ASIC.

   If you replied 'no' please explain why.

10. To what extent does your organisation review its internal complaints and dispute, and complaints that AFCA, or regulators, receive about or related to the organisation, for trends and emerging issues? Who carries out these analyses and what is done with the outcomes? If your organisation does not do so, please explain why.

11. For the quarter ending 30 June 2019 (Q4 2018–19), please provide us with the following information:

   a) The number and types of compliance incidents or breaches referred to your organisation's breach risk committee (or equivalent) as potentially significant or notifiable.

   b) The key outcomes of the breach risk committee's (or equivalent) assessment of the compliance incidents or breaches and its reasons, including:

      - Where applicable, why the breach risk committee did not consider the Code's significant breach criteria.
      - Where applicable, why the breach risk committee concluded that the compliance incident or breach was not a significant Code breach.
      - The number and types of compliance incidents or breaches that the breach risk committee reported to ASIC as a significant breach.

Note: If the breach risk committee did not consider any matters during Q4 2018–19, please complete this question for an earlier quarter and tell us which quarter your responses are about.

12. Would the breach risk committee deal with similar compliance incidents or breaches differently today under the Code? If yes, please describe what has changed.

13. What changes has your organisation made in response to the FSRC to improve Code compliance and operate in the spirit of Commissioner Hayne's six underlying principles reflecting norms of conduct?[24]

14. What lessons did your organisation take away from the FSRC?

15. What has your organisation done to implement changes in response to the lessons learned from the FSRC?

[24] Financial Services Royal Commission Final Report, pages 8 and 9.