INFORMATION PAPER

Self-assessments of governance, accountability and culture

22 May 2019

Disclaimer and Copyright

Contents

Executive summary

In May 2018, APRA released the Final Report of the Prudential Inquiry into the Commonwealth Bank of Australia (CBA). The Prudential Inquiry was launched following a series of significant operational and governance shortcomings that damaged the bank's reputation. The Final Report's major finding was that CBA's continued financial success had dulled the institution's senses, especially with regard to the management of non-financial risks.

The issues and incidents examined in the Final Report, coupled with findings of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (Royal Commission), highlight weaknesses in the management of non-financial risks – in particular, operational, compliance and conduct risks. When these risks materialise, they can result in significant financial consequences.

When the Final Report was released, APRA called on all APRA-regulated institutions to reflect on the findings and consider whether similar issues might exist in their own organisations. In addition, APRA wrote to the boards of 36 authorised deposit-taking institutions (ADIs), insurers and superannuation licensees asking them to conduct a self-assessment against the findings, and provide that assessment to APRA. APRA has since examined these self-assessments to assess their quality, identify common themes, and, where necessary, challenge institutions' findings.

APRA is releasing this Information Paper to assist institutions in understanding and addressing the challenges of embedding effective risk governance frameworks and practices. The paper discusses the outcomes of the self-assessment process, key findings and common themes, and some of the solutions being implemented by institutions. The paper also outlines the next phase of APRA's streams of work to strengthen prudential expectations and intensify supervision of governance, accountability and culture.

Overall, it is clear that the weaknesses identified in the Final Report of the Prudential Inquiry are not unique to CBA. A number of common themes have emerged from the self-assessments, including:

- non-financial risk management requires improvement;
- accountabilities are not always clear, cascaded and effectively enforced;
- acknowledged weaknesses are well-known and some have been long-standing; and
- risk culture is not well understood, and therefore may not be reinforcing the desired behaviours.

Most institutions critically examined their organisation, and have committed to a considerable list of actions. They have, however, generally rejected the notion that the cultural traits of complacency, insularity and collegiality underpinning the Prudential Inquiry findings are prevalent.

Significant uplift is required across industries to bring governance and the management of non-financial risks to an appropriate standard. This includes embedding robust frameworks that incentivise delivery of sound outcomes, proactive management of issues and consistent application of rewards and consequences. Boards and management are ultimately responsible for addressing weaknesses in their institution, and APRA will be holding them to account. Over the next 12 months, APRA will strengthen prudential expectations and increase supervisory intensity for governance, accountability and culture for all regulated institutions.

APRA is meeting with participating institutions and, as a next step, will be writing to the boards of each of the 36 institutions to provide feedback on their self-assessments, and outline APRA's intended targeted supervisory engagement. The nature of this engagement will depend on the quality and findings of the self-assessment, and the risk profile of the institution. One area of focus will be whether boards and senior leadership have been sufficiently self-critical given the wide range of weaknesses identified.

For some institutions, the issues identified in the self-assessment are material, and the changes required to address them are significant. APRA is therefore considering applying an additional operational risk capital requirement to reflect the higher risk profile of these institutions. To incentivise effective and timely rectification by institutions, this requirement would likely remain in place until issues are fully addressed.

Many institutions that conducted a self-assessment have developed plans to address the findings. While this is positive, a clear understanding of the underlying drivers of issues is essential. Absent this, institutions risk problems persisting or resurfacing in the future. APRA expects all regulated institutions to identify and address points of weakness and continues to encourage institutions that have not yet completed a thorough self-assessment to do so. Institutions should consider the observations in this paper when designing and implementing steps to enhance risk governance.

Glossary

APRA	Australian Prudential Regulation Authority
ADI	Authorised deposit-taking institution
CBA	Commonwealth Bank of Australia
CPS 220	*Prudential Standard CPS 220 Risk Management*
CPS 510	*Prudential Standard CPS 510 Governance*
CPS 520	*Prudential Standard CPS 520 Fit and Proper*
Final Report	Final Report of the Prudential Inquiry into the Commonwealth Bank of Australia
Prudential Inquiry	Prudential Inquiry into the Commonwealth Bank of Australia
Royal Commission	*Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry*
SPS 220	*Prudential Standard SPS 220 Risk Management*
SPS 510	*Prudential Standard SPS 510 Governance*

Overview

The Final Report of the Prudential Inquiry into the CBA found that continued financial success dulled the institution's senses to signals that might have otherwise alerted the Board and senior executives to a deterioration in the bank's risk profile.[1] This was particularly evident in relation to the management of non-financial risks.

The Prudential Inquiry also found a number of prominent cultural themes; there was a widespread sense of complacency, a reactive stance in dealing with risks, insularity and not learning from experiences and mistakes, and an overly collegial and collaborative working environment that lessened constructive criticism, timely decision-making and a focus on outcomes.

The Final Report listed 35 recommendations focussing on five key levers of change:

- more rigorous board and executive committee governance of non-financial risks;
- exacting accountability standards reinforced by remuneration practices;
- a substantial upgrading of the authority and capability of the operational risk management and compliance functions;
- injection of the "should we" question in relation to all dealings with and decisions on customers; and
- cultural change that moves the dial from reactive and complacent to empowered, challenging and striving for best practice in risk identification and remediation.

In releasing the Final Report, APRA noted that all regulated financial institutions would benefit from conducting a self-assessment to gauge whether similar issues might exist in their institutions. APRA subsequently wrote to the chairs of 36 institutions (refer to Attachment A) requesting a board endorsed written self-assessment of the effectiveness of their own governance, accountability and culture practices. APRA received all of the self-assessments by mid-December 2018.

Number of institutions requested to undertake self-assessments

ADI	General insurance	Life insurance	Private health insurance	Superannuation
9	9	4	3	11

APRA conducted a detailed review and benchmarking of the self-assessments to assess their quality, understand and challenge findings, and identify key themes. This forms an important

[1] Prudential Inquiry into the Commonwealth Bank of Australia – Final Report, 1 May 2018, available at: https://www.apra.gov.au/media-centre/media-releases/apra-releases-cba-prudential-inquiry-final-report-accepts-eu

component of APRA's ongoing program to strengthen industry practices and increase the intensity of risk governance supervision that also takes into account implementing relevant recommendations of the Royal Commission.

Quality of the self-assessments

APRA's request for institutions to conduct the self-assessments was intentionally not prescriptive. Boards were asked to determine an approach to the assessment which would provide them with a comprehensive understanding of the effectiveness of governance, accountability and culture, and enable them to form a view as to the extent the 'tone from the top' is permeating through and across the institution. As a result, the structure, methodology and format each institution took to completing the self-assessment was considered an important indicator of how seriously boards approached the task.

APRA set three principles that it expected the self-assessments to reflect:

- **Depth** – to enable the board to gain assurance that appropriate governance, accountability and culture are embedded in practices and behaviours, and enforced within the various levels and across the group-wide operations;
- **Challenge** – either independent or self-challenge, to provide the board with fresh perspectives on the strength of governance, accountability and culture (e.g. the assessment should not only reflect the view of the risk function); and
- **Insights** – to inform the board of areas requiring attention and improvement, and how better practice can be achieved.

Varied approaches

Most institutions recognised the opportunity provided by the findings in the Final Report to examine critically their own organisation. Some sought to replicate the Prudential Inquiry approach, incorporating case studies, board and senior leadership interviews, and staff surveys. Many institutions appointed external consultants to provide independent challenge in the self-assessment process and findings, while boards maintained an oversight role.

At the other end of the spectrum, a small number of institutions approached the self-assessment largely as an exercise for APRA rather than an opportunity to drive improvement. These institutions applied a lighter touch process, such as a "tick the box" approach, and justified this by indicating that the issues detailed in the Final Report could not and do not apply to them given the different scale or business models of their respective operations. This perspective is disappointing, particularly in light of the Prudential Inquiry's findings on the risks that arise from complacency. APRA continues to engage with institutions to seek greater insights on issues identified and additional evidence to support conclusions contained in the self-assessments.

Limited insight

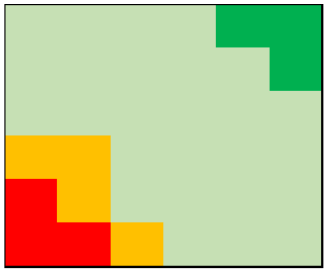
While most institutions met APRA's expectations for depth and challenge, only a few self-assessments identified new insights. Assessments often identified a range of weaknesses or opportunities to improve risk management practices; however, these were, in the main,

reported to be already known to boards and leadership teams. Notwithstanding the above, institutions recognised the benefit and importance of the self-assessment to provide an aggregate view of the issues in the organisation.

The extent of issues raised in self-assessments, accompanied with lengthy lists of planned actions, also suggests that many institutions have yet to develop a clear understanding of what factors have caused weaknesses to manifest and persist. It is important that boards and senior leadership appreciate why frameworks are not operating as intended and challenge themselves on whether proposed actions will be holistic and effective in delivering sustainable improvements in behaviours and practices.

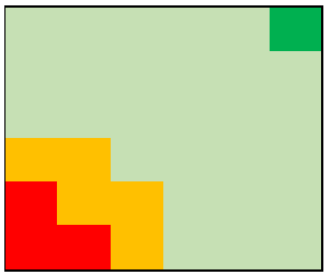
Figure 1: Quality of the self-assessments

Depth



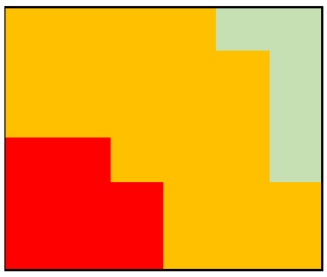
	Poor	Moderate	Good	Strong
ADI	0	1	8	0
Insurance	2	1	13	0
Superannuation	1	2	5	3
All entities	**3**	**4**	**26**	**3**

Challenge



	Poor	Moderate	Good	Strong
ADI	1	1	7	0
Insurance	1	1	14	0
Superannuation	1	3	6	1
All entities	**3**	**5**	**27**	**1**

Insights



	Poor	Moderate	Good	Strong
ADI	2	7	0	0
Insurance	3	9	4	0
Superannuation	3	7	1	0
All entities	**8**	**23**	**5**	**0**

Each square represents one institution. Ratings incorporate supervisory judgement and reflect APRA's view of whether the self-assessment met the objectives of depth, challenge and insights and provides a sound basis to improve practices.

- *Poor – Significant further work required to meet objective.*
- *Moderate – Some improvement required to meet objective.*
- *Good – Adequately addresses objective.*
- *Strong – Robust demonstration of objective.*

Weaker assessments on remuneration and culture

Although it was positive to see institutions' commitment to the self-assessments, APRA observed that self-assessments generally contained less detail on remuneration frameworks. While most self-assessments focused on remuneration design, few commented on the effectiveness of the framework as a whole. This included a lack of coverage of implementation, the use of board discretion in the remuneration process, the link between risk, conduct and customer outcomes and whether remuneration outcomes reflect policy intent.

Institutions' assessments of culture were also generally less comprehensive than other components in the self-assessments. Many institutions either struggled to articulate their assessment of culture or provided little evidence to support their assessment. While APRA acknowledges the challenges of measuring and analysing risk culture, it appears that there remains significant scope for improvement in this area.

Key findings

Findings from the self-assessments affirmed that embedding effective frameworks and controls to identify, manage and mitigate non-financial risks is a challenge for institutions regardless of size, complexity or industry. Specifically, APRA observed that:

- the weaknesses identified in the Prudential Inquiry are not unique to CBA;
- there are consistent findings relating to non-financial risk management, accountabilities, and risk culture; and
- institutions may not have fully identified the root causes of findings, resulting in the risk that actions to address weaknesses may not be effective or sustainable.

Comparisons to the Prudential Inquiry

The findings in the self-assessments demonstrate that the weaknesses identified by the Prudential Inquiry are, by and large, also apparent in other institutions. Almost all institutions acknowledged a range of shortcomings, albeit not to the same depth and extent as those stated in the Final Report. APRA observed a small number of self-assessments that were relatively positive about the effectiveness of governance, accountability and culture, identifying only minor opportunities for improvement, such as slight changes to meeting structure and attendees, or minor enhancements to board reporting and framework documentation.

The Final Report of the Prudential Inquiry presented 35 recommendations across eight topics:

- **Governance** (Role of the Board, Senior Leadership Oversight, Risk Management and Compliance, Issue Identification and Escalation, Financial Objectives and Prioritisation);
- **Accountability** (Accountability, Remuneration); and
- **Culture** (Culture and Leadership).

Many institutions set out their self-assessment findings in a comparable manner, identifying weaknesses across many of the eight topics. Institutions tended to have multiple findings and identified a more substantial need for improvement in Risk Management and Compliance, and Issue Identification and Escalation.

There were limited findings relating to the Role of the Board and Senior Leadership Oversight. Institutions largely rejected the notion that the cultural traits of complacency, insularity and collegiality underpinning the Prudential Inquiry findings are prevalent in their organisations.

Emerging themes

While the self-assessments exhibited considerable variation in the number and severity of findings, four themes emerged across all industries:

- *non-financial risk management requires improvement.* This was evidenced through a range of issues identified by institutions, including resource gaps (particularly in the compliance function), blurred roles and responsibilities for risk, and insufficient monitoring and oversight. Institutions acknowledged that historical underinvestment in risk management systems and tools has also contributed to ineffective controls and processes.

- *accountabilities are not always clear, cascaded, and effectively enforced.* Institutions noted that, while senior executive accountabilities are fairly well defined within frameworks, there is less clarity or common understanding of responsibilities at lower levels, and points of handover where risks, controls and processes cut across divisions. This is further undermined by weaknesses in remuneration frameworks and inconsistent application of consequence management.

- *acknowledged weaknesses are well known and some have been long-standing.* The majority of self-assessment findings were reported to be already known to boards and senior leadership. Nevertheless, some issues have been allowed to persist over time, with competing priorities, resource and funding constraints typically cited as the basis for acceptance of slower progress. It was observed that these issues are often only prioritised when there is regulatory scrutiny or after adverse events.

- *risk culture is not well understood, and therefore may not be reinforcing the desired behaviours.* Institutions are putting considerable effort into assessing risk culture, but many continue to face difficulties in measuring, analysing, and understanding culture (and sub-cultures across the institution). It is therefore unclear if these institutions can accurately determine whether their culture is effectively reinforcing desired behaviours (or identify how it would need to be changed to do so).

While the self-assessments contained some in-depth self-reflection and acknowledgement by institutions of issues within their organisations, the assessments relating to the effectiveness of boards and senior leadership were notably less critical. Many self-assessments noted that the institution is generally well governed, with a respected and suitably challenging board, strong executive leadership teams and a good tone from the top, although at the same time acknowledging weaknesses spanning most or all chapters of the Final Report. This raises the question of whether boards and senior management have a potential blind spot when it comes to assessing their own effectiveness.

These themes are discussed further under *Themes from the self-assessments*.

Execution risks

The self-assessments present an opportunity to strengthen risk governance practices and rebuild public trust at a time when institutional reputations in the financial sector have been damaged. To achieve this, there needs to be a well-considered and prioritised plan that effectively targets the underlying causes of the identified weaknesses.

APRA observed that self-assessments generally focused on symptoms without adequate consideration of the underlying drivers. Therefore, while most institutions have developed and committed to a list of actions, or have initiatives in train, there is a risk that these activities may not address the issues effectively or sustainably.

Many self-assessments, particularly those of the larger institutions, also identified weaknesses in program delivery, including for risk-related projects. Institutions recognised tendencies for delays and changes in the scope of projects, and a lack of accountability for outcomes. Some of the largest institutions also acknowledged a propensity to cultivate complexity in what they do – systems, processes and policies – which hinders effective execution. This suggests further risks to effective execution of plans to address weaknesses.

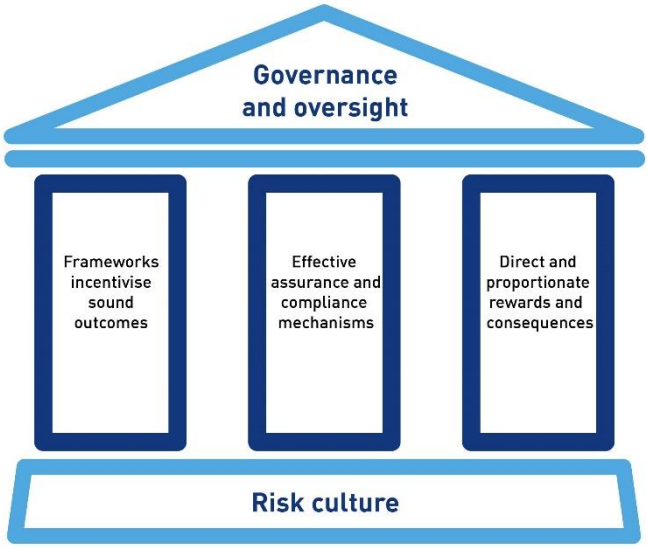
Themes from the self-assessments

The importance of risk governance was well recognised in the wake of the Global Financial Crisis, reflecting its social and economic cost. While this led institutions to significantly lift their focus on financial risks, including capital, liquidity, credit and market risks, the same discipline was not universally applied to non-financial risks. The Prudential Inquiry and findings of the Royal Commission further reinforced that a trusted financial sector also requires strong governance of non-financial risks.

Strong governance and risk management frameworks would typically exhibit:

- accountability and remuneration frameworks that incentivise delivery of sound outcomes, in particular executive remuneration that is designed to better align rewards with a holistic view of performance;
- effective assurance and compliance mechanisms that drive proactive monitoring, early detection and escalation, and timely rectification of issues; and
- direct and proportionate rewards and consequences that are consistently applied to hold individuals to account for financial and non-financial outcomes.

***Figure 2:** Risk governance architecture*



To be effective, these elements need to be supported by strong governance and risk oversight, and driven by a sound risk culture. In discharging their oversight function, boards must regularly challenge, and seek assurance and evidence of whether frameworks are operating as intended to deliver the targeted risk and customer outcomes. Senior leadership should also pay attention to the institution's risk culture, and the extent to which it aligns with risk appetite and is reinforcing the desired behaviours.

The self-assessments indicate that institutions have a significant undertaking ahead to lift risk governance to the necessary standard. It is ultimately the responsibility of boards and senior leadership to implement these actions effectively. APRA will also strengthen its prudential framework and increase supervisory intensity of governance, accountability and culture to drive improvement across the sector.

Most institutions have committed to a range of actions to address the weaknesses acknowledged in their self-assessments. This section of the paper includes a sample of these specific commitments that may be relevant to other institutions as they undertake steps to enhance risk governance.

Non-financial risk management requires improvement

Institutions assessed that, while the oversight of financial risks is generally considered to be strong, non-financial risk management is less mature, reflecting that it has traditionally not been regarded with the same importance. Across industries, there is more to be done to improve the effectiveness of operational, compliance and conduct risk frameworks.

***Figure 3:** Weaknesses in non-financial risk management*

Some common issues identified include blurring of roles and responsibilities for non-financial risk management, compounded by shortages in skills and headcount. The tendency to prioritise financial risks has also meant that non-financial risks do not get the appropriate level of visibility. This in turn influences investment decisions and contributes to control weaknesses.

Blurred roles

Many self-assessments acknowledged challenges in consistently applying the 'three lines of defence' model. Despite risk management frameworks being in place for many years, practices are yet to be fully embedded within many institutions.

Although risk management frameworks have sought to define roles and responsibilities across the three lines of defence, institutions acknowledged they continue to be blurred in practice. This blurring is particularly evident between first and second line functions. One institution noted "inconsistency in the application of the three lines of defence model..... (with) variability in the capability, resources, roles and responsibilities of the first and second lines". Most self-assessments also pointed to a lack of risk ownership by first line leading to second line stepping in and conducting first line risk activities, which limits the ability to undertake comprehensive risk and assurance activities.

Many institutions, particularly in the banking and insurance industries, also noted room to elevate the organisational status and influence of the risk and compliance functions. This requires an uplift in skills and headcount; a widely recognised issue due to heightened market competition for experienced risk and compliance personnel. This view was not shared as strongly by superannuation institutions.

Control weaknesses

Institutions recognised that risk management frameworks have not been implemented effectively. Many self-assessments noted gaps, including control weaknesses that are magnified by complex systems and processes.

Self-assessments identified numerous factors contributing to control weaknesses. Most institutions have further work ahead to understand end-to-end processes across their businesses, with this being a pre-requisite to the development of a robust and detailed understanding of the control framework. Self-assessments noted inconsistent and reactive risk identification processes which could lead to control gaps not being proactively managed. They also indicated weaknesses in control frameworks, including in data quality and control classification and assessment processes. One institution identified examples where "controls have been incorrectly assessed or do not effectively manage the risks identified". Another institution noted that "a relatively high proportion of controls have not been validated on time".

There was also an apparent acceptance of untimely and reactive resolution, with a propensity for short-term tactical fixes rather than long-term strategic solutions. One institution noted an (unfortunate) "emphasis on creating more activity rather than understanding the root-cause, specifically when things have gone wrong".

Poor visibility of issues

Many institutions recognised the need to improve data, measurement and reporting for non-financial risks. Insufficient data, coupled with system and process limitations, have impaired institutions' ability to identify emerging or systemic risks, escalate and manage issues, and analyse why sub-optimal risk and customer outcomes have occurred.

One institution noted "There is no consolidated report which brings together all key audit, risk, regulatory and customer issues requiring resolution to enable a holistic view of all remediation work required and the status thereof.....no periodic or structured analysis of all relevant data.....to facilitate deeper root-cause analysis". For some large institutions, these weaknesses contributed to significant regulatory compliance breaches. Self-assessments noted delayed identification of incidents, and failure to report breaches within regulatory timeframes.

Institutions also acknowledged that indicators and metrics for measuring and monitoring non-financial risks are fairly basic, compromising the ability for robust internal challenge. It appears that standalone monitoring of 'conduct risk' is relatively new, often with a focus on the customer 'net promoter score', with no analysis or reporting of complaints data that could be used as a lead indicator. Some institutions simply noted an intention to improve conduct risk management practices.

A large number of self-assessments also pointed to voluminous board and committee reporting, which did not always highlight key risks that required closer attention from directors. Poor data analytics capabilities, as discussed above, have also hampered the ability to report insights to support challenge and decision-making. As an example, a case study cited by one institution relating to an incident found that reporting to executive committees

and the board was predominantly focused on technological aspects of the incident and offered little information on the negative customer impact.

Examples of institution actions to strengthen non-financial risk management:

"Clarify roles and responsibilities across 3 LOD.....and role and responsibility mapping (including across end-to-end processes), to ensure that.....the 3 LOD model is consistent across divisions."

"Strengthening risk capability across all Three Lines of Defence with a focus on conduct, root cause analysis, and strengthening the voice of risk."

"Establish an Executive Risk Committee for oversight and accountability over material risk strategies, treatments and outcomes."

"Incorporate incident, complaints, voice of customer and internal audit data requirements into the customer relationship management system and the data warehouse."

"Improve the reporting.....to include remediation status of high rated and long-outstanding issues, metrics on open issues with ageing, the residual risk during remediation, a regular assessment of whether the matter is being addressed in a timely manner and details of appetite breaches for non-financial risk."

Accountabilities are not always clear, cascaded and enforced

There was broad recognition that accountabilities for non-financial risk management could be strengthened. Risk ownership and accountabilities should be better defined, and supported through remuneration frameworks and consequence management practices.

***Figure 4:** Weaknesses in accountability frameworks and practices*

Accountabilities are not always clear

Self-assessments acknowledged that accountabilities for non-financial risks were not always clearly understood. This was particularly evident where risks, controls and processes span multiple business units or divisions. One self-assessment stated that "there have been challenges in establishing clarity around roles and accountabilities and end-to-end ownership of processes". Another self-assessment noted that "the executive governance framework is inconsistent and varies in operational effectiveness.....this can lead to confusion or gaps over functional coverage, issue escalation and decision making".

Larger institutions cited organisational and process complexity, including multiple forums and committees, as key factors confusing accountabilities. The rate of change facing many institutions, internally and in the external operating environment, also exacerbated the

challenge of embedding clear accountabilities. One institution noted that accountability for addressing an issue was segregated into separate and discrete actions, and assigned to different leaders. When the issue remained open and was reviewed several years later, it was found that there had been multiple changes in issue ownership, and all of the initial accountable leaders had left the institution. Institutions also noted a reliance on informal networks for resolving incidents.

Implementation of the Banking Executive Accountability Regime (BEAR) for ADIs has been credited with clarifying accountabilities for the most senior executives, and other industries refer to the regime as a means to sharpen executive accountability.[2] A number of self-assessments noted the intention to cascade and embed the principles of the BEAR throughout the institution.

Rigour of consequence management

Self-assessments generally acknowledged the need to enhance consequence management. This requires the application of direct and proportionate consequences to hold individuals to account when issues emerge and are not promptly addressed.

Many self-assessments also recognised inconsistencies in the way consequences were applied across business units and at different levels of seniority. One institution noted that "while ageing of audit items is monitored and owners are identified, individuals are not consistently held to account for the lack of timely resolution of issues". Other institutions highlighted variations in the frequency of non-remuneration consequences between divisions, back and front office functions, and staff levels.

Remuneration and risk misaligned

As previously noted, self-assessments generally contained less detail on the effectiveness of remuneration frameworks. APRA observed that further work is required to ensure risk and customer objectives are reflected in remuneration outcomes, with gaps evident between current remuneration frameworks and better practices as set out by APRA and international bodies. Based on information in self-assessments, most institutions are yet to address fully the findings from APRA's 2018 information paper *Remuneration Practices at Large Financial Institutions* or incorporate the Financial Stability Board's *Principles and Standards on Sound Compensation Practices (including the Supplementary Guidance addressing misconduct risk)*.[3] While some institutions have started to address these findings, progress appears slow and some material gaps remain.

---

[2] The BEAR commenced for large ADIs on 1 July 2018 and will commence for remaining ADIs on 1 July 2019.

[3] APRA, *Remuneration Practices at Large Financial Institutions*, 4 April 2018, available at: https://www.apra.gov.au/media-centre/media-releases/apra-seeks-improvement-executive-remuneration-practices

Financial Stability Board, *Supplementary Guidance to the FSB Principles and Standards on Sound Compensation Practices*, March 2018, available at: http://www.fsb.org/2018/03/supplementary-guidance-to-the-fsb-principles-and-standards-on-sound-compensation-practices-2/

High level observations from the self-assessments included:

- some institutions recognised a need for stronger board oversight and challenge of remuneration outcomes;
- risk information provided to the board remuneration committee for remuneration purposes appeared to be at a high level without a clear link to the institution's broader approach to risk management;
- while non-financial metrics were commonly included in scorecards, it appeared that a disproportionate focus was placed on the achievement of financial metrics;
- the level of input by the risk function and the board risk committee (or equivalent) into the risk assessment component in scorecards remained limited for most institutions; and
- guidelines for the use of adjustment tools such as malus and clawback need development.

These observations raise questions about the rigour applied in assessing the effectiveness of remuneration frameworks, including back-testing of outcomes, as required under *Prudential Standard CPS 510 Governance* (CPS 510) and *Prudential Standard SPS 510 Governance* (SPS 510). These reviews should assist institutions in identifying weaknesses in their frameworks, including those outlined above.

Examples of institution actions to clarify and enforce accountabilities:

".....embed accountability principles and practices.....so that leaders beneath the Executive Leadership Team have an equally clear understanding of their responsibilities and expectations of them."

"Review the approach to consequence management to provide greater guidance on and allow better consolidation of outcomes."

".....Group Executive scorecards to include progress in reduction of long-dated complaints or similar metric that attaches accountability for the resolution of matters....."

"Produce aggregated data showing the size of, and reasons for, remuneration adjustments by division for consideration by relevant committees and functional areas."

".....improve oversight of remuneration outcomes, particularly as they relate to risk assessment and remuneration consequence. This will include.....increased expectations of documentation and data submitted.....and the documentation of considerations and outcomes."

Acknowledged weaknesses are already known

Many institutions acknowledged that the findings in self-assessments were known issues. They therefore generally did not consider the specific findings to be surprising, although many noted that the issues in aggregate were confronting.

The majority of self-assessments noted that actions are underway to address many of the findings. While this is positive, it is still concerning that weaknesses have been tolerated. A number of factors appear to be contributing to these persistent issues.

***Figure 5:** Factors contributing to persistent issues*

Ineffective solutions

Some institutions recognised issues of reactivity in non-financial risk management. It is not uncommon for issues to receive focus and prioritisation only when they come under regulatory scrutiny, or after an event materialises. Some institutions also acknowledged a tendency to apply tactical fixes to issues rather than implement more strategic solutions, resulting in rectification that is not always effective, with issues subsequently recurring.

Self-assessments pointed to various reasons for weak implementation of solutions, including inadequate root-cause analysis and poor identification of systemic issues. For some institutions, investment prioritisation was also influenced by a focus on short-term results rather than long-term sustainability. Some self-assessments recognised the need for elevation of the voice of risk (and of customers/fund members) in the funding prioritisation process.

A number of large institutions also acknowledged a tendency to cultivate complexity, including in designing and implementing solutions. This has implications for project execution (for example, de-scoping or failure to fully execute), that are compounded by legacy systems and system constraints.

Insufficient information and challenge

There was broad acknowledgement in self-assessments that non-financial risks have not received adequate attention and that the quality of information and reporting could be improved. A number of larger institutions also noted that voluminous reporting could be better targeted to highlight key insights and issues requiring closer attention, with more focus placed on underlying assumptions and risks (including risks associated with investment allocation).

The materiality of non-financial risk consequences may not be adequately understood or receiving the right level of visibility. In turn, this is likely to be contributing to a 'boiling frog' effect, where issues are tolerated and action is only prioritised when there is regulatory scrutiny or after adverse events.

Examples of institution actions to improve issues management:

"Review Board and committee papers to ensure they have the right level of detail, important issues are appropriately highlighted, unnecessary duplication is removed and visibility and oversight of audit points and action items is appropriate."

"Address organisational complexity and legacy risk by simplifying group structures, product offerings and related systems."

"The Board will require and oversee enhancements to non-financial risk reporting, in particular to ensure key matters are escalated early and clearly and that adequate agenda time is allocated to them."

"Ensure executive ownership and engagement in divisional and group committees with consistent reporting and analysis of current risks, issues and incidents and emerging risks."

"Accountable Group Executives will be invited to.....meetings to speak to audit findings, issues and incidents."

Risk culture is not always well understood

When APRA published its information paper *Risk Culture* in 2016, it observed that approaches by institutions to understand and manage risk culture were at a relatively early stage of development: efforts had mainly focused on the initial task of defining, understanding and assessing the institution's current state of risk culture.[4]

***Figure 6:** Shortcomings in assessing and understanding risk culture*

Despite focus on culture increasing in recent years, the quality of institutions' self-assessments indicates to APRA that significant scope for improvement and investment remains. As expected, approaches

[4] APRA, *Risk Culture*, 18 October 2016, available at: https://www.apra.gov.au/media-centre/media-releases/apra-releases-snapshot-industry-practice-risk-culture

to assessing and understanding risk culture varied by institution size, business mix and complexity.

Measurement and analysis of culture is still developing

APRA observed that many institutions tended to rely on surveys as a single source of data to support self-assessment findings on culture, often forming broad conclusions based on a limited set of culture-related questions added to a more general staff survey. There were limited attempts by institutions to validate survey results with results from multiple data sources.

There are many ways that institutions could measure, analyse and draw insights on risk culture. More advanced approaches would combine data from a variety of sources to arrive at well-substantiated, evidence-based conclusions. This could include the use of surveys, workshops, focus groups, risk culture audits and interviews, conducted by either independent internal resources or external consultants.

There is varied, but overall insufficient, regularity of reporting to the board on risk culture issues, and limited efforts to link risk culture outcomes to stated risk appetite. Risk culture assessments should place more focus on the extent to which the institution is operating consistently within its risk appetite.

Behaviours overlooked in favour of formal mechanisms

Actions identified in self-assessments focused primarily on addressing processes and systems, without due attention to the culture and behaviours required to make such systems produce the desired outcomes. Solutions tended to target legacy systems issues, insufficient data and reporting, and inadequate documentation of processes, rather than communication, decision-making and leadership. Only a minority of self-assessments identified the need to address behaviours such as fear of speaking up and failure to listen to the voice of the customer (such as customer complaints), which are useful indicators of cultural problems in an institution.

A number of institutions also identified complexity as a limit to improving risk culture. In one example, operational and regulatory complexity and an "inherently complex organisational structure" were repeatedly cited as explanations for sub-optimal outcomes, without sufficient consideration of risk culture. While complexity presents challenges to achieving a desired risk culture, institutions should be cognisant of a 'too hard' mindset becoming a barrier to effecting cultural change.

Lack of a clear view of risk culture

As set out in *Prudential Standard CPS 220 Risk Management* (CPS 220), APRA expects boards to form a view of the risk culture in the organisation, and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite.[5] A small

[5] CPS 220 applies to ADIs, general insurers, life companies and private health insurers. In superannuation the equivalent standard, *Prudential Standard SPS 220 Risk Management* (SPS 220), provides that an RSE licensee has responsibility to ensure that all persons within the business operations have awareness of the risk management framework and for instilling an appropriate risk culture across the RSE licensee's business operations.

number of self-assessments sought to draw links between values, culture and risk appetite, demonstrating a higher level of maturity in assessing and understanding culture. That said, few institutions were able to characterise their risk culture, seeking only to disassociate from the traits specified in the Final Report.

Very few self-assessments were able to articulate a target culture or express views on whether they were close to achieving the desired culture. Those that did typically demonstrated a strong understanding of the drivers of behaviour and a recognition that culture is central to business models and effective strategy. They also exhibited an appreciation of how boards and leadership teams can influence risk culture. For example, one self-assessment emphasised the need for "enhancement of leadership skills" to improve its risk culture, particularly by effectively communicating lessons learnt. Another self-assessment was able to articulate what the board considered to be acceptable and unacceptable behaviours. This institution noted culture as one of the most material risks for the organisation and a key driver of good decision-making and strategic success.

Examples of institution actions to improve assessment of risk culture:

".....will improve the links between risk and broader culture initiatives, clarify the roles and responsibilities for risk culture measurement and monitoring across the 3LoD, and embed effective metrics and tools to support assessment and reporting, including validating its assessment of risk culture against other data points."

"The Board should continue to explore and develop additional quantitative and qualitative information and reporting on culture."

".....develop risk culture metrics and reporting.....to facilitate monitoring and understanding of risk culture and update the risk appetite framework, including reporting dashboards, to support the enhanced articulation of non-financial risk appetite."

"Ensure adequate and sustained focus on improving culture through a range of initiatives, including continuing the tone from the top on communicating the importance of strong risk management, open environment for raising issues, and non-acceptance of changing/unclear processes as reasons for events."

"Develop a Board communication plan and calendar to support CEO messaging and to reinforce direct 'tone from the top' (reinforcing and leveraging our existing values....."

The way forward - intensifying supervision of governance, accountability and culture

Ultimately the responsibility for risk culture, and embedding strong frameworks and practices to deliver outcomes, rests with boards and senior leadership of regulated institutions. APRA cannot regulate good culture into existence, or design and implement strong frameworks for institutions.

APRA does however have a role to play to provide a sound foundation and reinforce effective practices. To that end, APRA will strengthen and clarify its prudential framework, and concurrently broaden and deepen the scope and intensity of supervision. Under its newly adopted "constructively tough" enforcement appetite, APRA will also use its formal enforcement powers and the full extent of its toolkit as and where necessary to hold institutions and individuals to account.[6]

APRA is directing additional resources to a multi-year effort involving inter-related streams of work to intensify supervision of governance, accountability and culture. This program is informed by supervisory activities, the findings from the Prudential Inquiry, APRA's review of remuneration practices, analysis of the self-assessments, and directed to addressing the recommendations arising from the Royal Commission.

APRA has committed to enhancing its approach to supervision of risk culture and work is underway to develop capacity and capability in this regard.[7] The enhanced approach involves:

- adopting a risk-based approach to conducting risk culture reviews across a wide range of institutions;
- scoping these reviews to include consideration of the influence of risk culture on non-financial risk management, which may involve cases of misconduct; and
- stronger and more direct engagement with boards and senior leadership to hold them to account for actions to address identified risks.

APRA's immediate focus is engagement with those institutions that undertook a self-assessment. Some institutions were not formally requested to conduct a self-assessment, but did so voluntarily. Others that have not yet chosen to undertake such a process are encouraged to do so, given the value derived from identifying and addressing important points of weakness before problems crystallise in the form of poor business or customer outcomes.

---

[6] APRA, *APRA's Enforcement Approach* and *Enforcement Strategy Review,* 16 April 2019, available at: https://www.apra.gov.au/media-centre/media-releases/apra-releases-new-enforcement-approach

[7] APRA, *APRA update on implementation of Royal Commission recommendations* (refer to recommendation 5.7), 11 February 2019, available at: https://www.apra.gov.au/media-centre/media-releases/apra-update-implementation-royal-commission-recommendations

Engaging with boards and senior leadership teams

APRA is meeting with institutions that undertook a self-assessment to provide feedback and will also be writing to each of the 36 institutions to outline specific observations and next steps in supervisory engagement. The extent and nature of engagement with, and the resulting supervisory strategy for, each institution will vary depending on factors such as the quality and findings of the self-assessment, the risk profile of the institution and the extent to which the institution's action plan is considered susceptible to execution risk.

For some institutions, the issues identified in the self-assessment are significant, and the changes required to address them are material, presenting a heightened operational risk. To reflect this, APRA is considering the need for the application of an additional operational risk capital requirement until issues are fully addressed. Linking this capital overlay to action plans provides an additional incentive for institutions to pursue timely and effective rectification, where this has previously proved challenging.

APRA will also consider the extent to which further targeted thematic reviews may be required to continue to drive improvements in governance, accountability and culture across the financial services sector.

APRA's policy agenda

APRA's policy agenda for the next 12 months includes strengthening prudential expectations for governance, accountability and culture.[8] In particular:

- APRA will update its requirements for remuneration to focus on better alignment of remuneration, prudent risk management outcomes and long-term financial soundness, recognising the need to ensure incentives within financial institutions promote high standards of conduct and management of non-financial risks. APRA will consult on a new prudential standard on remuneration in mid-2019.

- as recommended by the Royal Commission, with the Government APRA has commenced planning for an extension of the BEAR to all APRA-regulated sectors, as well as a broadening of the scope to address product management and customer remediation. APRA will also align and integrate the legislative requirements under BEAR with the broader prudential framework, and will consult on updates to the existing fit and proper requirements in *Prudential Standard CPS 520 Fit and Proper*.

- APRA will also review and clarify the governance and risk management provisions set out in CPS 510 and CPS 220 to ensure they remain fit for purpose. This includes more clearly articulating APRA's expectations of boards and senior management.

[8] APRA, *APRA's Policy Priorities,* 28 February 2019, available at: https://www.apra.gov.au/media-centre/media-releases/apra-announces-policy-priorities-2019

Attachment A - Institutions requested to conduct a self-assessment

ADI	Australia and New Zealand Banking Group Limited Bank of Queensland Limited Bendigo and Adelaide Bank Limited Credit Union Australia Ltd Cuscal Limited Macquarie Bank Limited National Australia Bank Limited Teachers Mutual Bank Limited Westpac Banking Corporation
General insurance	Allianz Australia Insurance Limited Chubb Insurance Australia Ltd Genworth Financial Mortgage Insurance Pty Limited The Hollard Insurance Company Pty Ltd Insurance Australia Limited Munich Reinsurance Company QBE Insurance (Australia) Limited Suncorp Group Limited Swiss Reinsurance Company Ltd
Life insurance	AMP Life Limited Challenger Life Company Limited MLC Limited TAL Life Limited
Private health insurance	Australian Unity Health Limited NIB Health Funds Ltd Westfund Limited
Superannuation	AustralianSuper Pty Ltd Commonwealth Superannuation Corporation Diversa Trustees Limited

First State Super Trustee Corporation
Mercer Superannuation (Australia) Limited
Perpetual Superannuation Limited
QSuper Board
Retail Employees Superannuation Pty. Limited
Sunsuper Pty. Ltd.
United Super Pty Ltd (trustee for Construction & Building Unions Superannuation)
Host-Plus Pty. Limited

APRA